Upgrading to LiveCycle® ES for WebSphere®

Adobe® LiveCycle® ES

July 2007

Version 8.0

© 2007 Adobe Systems Incorporated. All rights reserved.

Adobe® LiveCycle® ES (8.0) Upgrading to LiveCycle ES for WebSphere® for Microsoft® Windows®, UNIX®, and Linux
Edition 1.1, July 2007

If this guide is distributed with software that includes an end user agreement, this guide, as well as the software described in it, is furnished under license and may be used or copied only in accordance with the terms of such license. Except as permitted by any such license, no part of this guide may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, recording, or otherwise, without the prior written permission of Adobe Systems Incorporated. Please note that the content in this guide is protected under copyright law even if it is not distributed with software that includes an end-user license agreement.

The content of this guide is furnished for informational use only, is subject to change without notice, and should not be construed as a commitment by Adobe Systems Incorporated. Adobe Systems Incorporated assumes no responsibility or liability for any errors or inaccuracies that may appear in the informational content contained in this guide.

Please remember that existing artwork or images that you may want to include in your project may be protected under copyright law. The unauthorized incorporation of such material into your new work could be a violation of the rights of the copyright owner. Please be sure to obtain any permission required from the copyright owner.

Any references to company names, company logos and user names in sample material or sample forms included in this documentation and/or software are for demonstration purposes only and are not intended to refer to any actual organization or persons.

Adobe, the Adobe logo, Acrobat, FrameMaker, LiveCycle, PageMaker, PhotoShop, and Reader are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States and/or other countries.

IBM, AIX, DB2, and WebSphere are trademarks of International Business Machines Corporation in the United States, other countries, or both.

Linux is the registered trademark of Linus Torvalds in the U.S. and other countries.

Microsoft and Windows are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Oracle is a trademark of Oracle Corporation and may be registered in certain jurisdictions.

Sun, Solaris, and Java are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and other countries.

UNIX is a registered trademark of The Open Group in the US and other countries.

All other trademarks are the property of their respective owners.

This product contains either BISAFE and/or TIPEM software by RSA Data Security, Inc.

This product includes software developed by the Apache Software Foundation (http://www.apache.org/).

This product includes code licensed from RSA Data Security.

This product includes software developed by the JDOM Project (http://www.jdom.org/).

Macromedia Flash 8 video is powered by On2 TrueMotion video technology. © 1992-2005 On2 Technologies, Inc. All Rights Reserved. http://www.on2.com.

This product includes software developed by the OpenSymphony Group (http://www.opensymphony.com/).

Portions of this code are licensed from Nellymoser(www.nellymoser.com)

MPEG Layer-3 audio compression technology licensed by Fraunhofer IIS and THOMSON Multimedia (http://www.iis.fhg.de/amm/).

This product includes software developed by L2FProd.com (http://www.L2FProd.com/)

The BeanShell library is licensed under the GNU Library General Public License, a copy of which is included with this software.

This product includes software developed by The Werken Company.

This product includes software developed by the IronSmith Project (http://www.ironsmith.org/).

The OpenOffice.org library is licensed under the GNU Library General Public License, a copy of which is included with this software.

Adobe Systems Incorporated, 345 Park Avenue, San Jose, California 95110, USA.

Notice to U.S. Government End Users. The Software and Documentation are “Commercial Items,” as that term is defined at 48 C.F.R. §2.101, consisting of “Commercial Computer Software” and “Commercial Computer Software Documentation,” as such terms are used in 48 C.F.R. §12.212 or 48 C.F.R. §227.7202, as applicable. Consistent with 48 C.F.R. §12.212 or 48 C.F.R. §§227.7202-1 through 227.7202-4, as applicable, the Commercial Computer Software and Commercial Computer Software Documentation are being licensed to U.S. Government end users (a) only as Commercial Items and (b) with only those rights as are granted to all other end users pursuant to the terms and conditions herein. Unpublished-rights reserved under the copyright laws of the United States. Adobe Systems Incorporated, 345 Park Avenue, San Jose, CA 95110-2704, USA. For U.S. Government End Users, Adobe agrees to comply with all applicable equal opportunity laws including, if appropriate, the provisions of Executive Order 11246, as amended, Section 402 of the Vietnam Era Veterans Readjustment Assistance Act of 1974 (38 USC 4212), and Section 503 of the Rehabilitation Act of 1973, as amended, and the regulations at 41 CFR Parts 60-1 through 60-60, 60-250, and 60-741. The affirmative action clause and regulations contained in the preceding sentence shall be incorporated by reference.

Contents

About This Document 5
What's in this document? 5
Who should read this document? 6
Additional information 6
Conventions used in this guide 6

1 Introduction 8
About installing, configuring, and deploying LiveCycle ES 8
About upgrading 9
How the LiveCycle upgrade works 9
Post-deployment upgrade tasks 10
Updating client applications 10
Updating LiveCycle QPACs 11
Selecting tasks for configuring and deploying LiveCycle ES 11
Installation, configuration, upgrading, and deployment checklists 12
Automatic installation and deployment checklist 12
Manual installation and deployment checklist 13

2 Installing the Solution Component Files 15
Installing Acrobat for LiveCycle PDF Generator ES 15
Installing LiveCycle ES 16
Viewing the error log 19
Specifying class path and JAVA_HOME 19
Next steps 20

3 Manually Configuring WebSphere 21
Configuring the JVM arguments and properties 21
Configuring WebSphere time-out settings 22
Increasing transaction time-out and ORB service values for PDF Generator ES 23
Configuring throttling for LiveCycle PDF Generator ES 24
Configuring the LiveCycle ES database connectivity 24
Configuring the DB2 data source 25
Configuring the Oracle data source 28
Configuring the SQL Server data source 30
Configuring JMS resources for WebSphere 34
Assigning JMS Activation Specification 37
Configuring J2C authentication for JMS 39
SQL Server JMS validation 40
Restart WebSphere 40
Next step 41

4 Configuring LiveCycle ES for Deployment 42
About LiveCycle Configuration Manager 42
Determining the application server SOAP port 43
Configuring, upgrading to, and deploying LiveCycle ES 43
Manually deploying the EAR files 50
Uninstalling EAR files 51
Next steps 52

5 Post-Deployment Activities 53
Verifying the deployment and accessing LiveCycle Administration Console 53
Accessing LiveCycle Administration Console 53
Viewing the log files 54
Deleting working files that contain sensitive data 54
Configuring Acrobat 8.1 for PDF Generator ES 55
Final setup for LiveCycle Rights Management ES 55
Upgrading to LiveCycle Business Activity Monitoring ES 55
Accessing User Management 56
Accessing solution component web applications 57
Accessing LiveCycle Rights Management ES 57
Migrating HSM credentials 58
Enabling FIPS mode 59
Configuring LiveCycle ES to access LDAP 60
Configuring HTML digital signature 60
Configuring the Connector for EMC Documentum service 61
Creating the XDP MIME format in your Documentum repository 63
Configuring the Connector for IBM FileNet service 64
Setting the Adobe PDF Printer as default for PDF Generator ES 67
Setting environment variables for PDF Generator ES 67
Setting PDF Generator ES watched folder performance parameters 68
Verifying that all languages are displayed after conversion with PDF Generator ES 68
Creating email endpoints for email notifications 69
Uninstalling LiveCycle ES 69

A Troubleshooting 70
Getting help 70
Installation considerations 70
Application server considerations 70
Database initialization considerations 71
Troubleshooting with log files 71
LCM log file 71
Viewing the JVM system output and error logs 71
Modifying WebSphere log level 72
Error messages 72
Class not found 72
JNDI name not found 72
J2CA0294W warning messages 73
Exceptions thrown when initializing the LiveCycle ES database multiple times 73
LiveCycle Policy Server to LiveCycle Rights Management ES 73
Additional upgrade issues 74

Index 76

About This Document

This document is one of several resources available to help you learn about upgrading to Adobe® LiveCycle® ES (Enterprise Suite) from Adobe LiveCycle 7.x products.

What's in this document?

This document provides information about how to upgrade from the following LiveCycle 7.x products to the corresponding LiveCycle ES solution components on Microsoft® Windows®, Linux®, IBM® AIX®, and Sun™ Solaris™, and how to deploy the solution components to a IBM® WebSphere® Application Server:

Adobe LiveCycle 7.x products	**Adobe LiveCycle ES solution components**
Adobe LiveCycle Document Security	Adobe LiveCycle Digital Signatures ES
Adobe LiveCycle Form Manager	Adobe LiveCycle Workspace ES
Adobe LiveCycle Forms (with or without User Management and Administrator)	Adobe LiveCycle Forms ES
Adobe LiveCycle PDF Generator	Adobe LiveCycle PDF Generator ES
Adobe LiveCycle Print	Adobe LiveCycle Output ES
Adobe LiveCycle Policy Server	Adobe LiveCycle Rights Management ES
Adobe LiveCycle Reader Extensions	Adobe LiveCycle Reader Extensions ES
Adobe LiveCycle Workflow	Adobe LiveCycle Process Management ES
Adobe LiveCycle Workflow Business Activity Monitor	Adobe LiveCycle Business Activity Monitoring ES
Adobe LiveCycle Assembler	Adobe LiveCycle PDF Generator ES (or Adobe LiveCycle Forms ES or Adobe LiveCycle Output ES. For information, see *Preparing to Upgrade to LiveCycle ES* at http://www.adobe.com/go/learn_lc_upgradePreparation.)

You do not need to refer to the *Installing and Deploying LiveCycle ES* documents if you are upgrading to LiveCycle ES. This document, combined with *Preparing to Upgrade to LiveCycle ES* at http://www.adobe.com/go/learn_lc_upgradePreparation, contains all the information you need to upgrade LiveCycle 7.x to LiveCycle ES.

Who should read this document?

This document provides information for administrators or developers responsible for upgrading to LiveCycle ES components. The information provided is based on the assumption that anyone reading this document is familiar with Java™ 2 Platform, Enterprise Edition (J2EE) application servers, Linux, Windows, AIX, or Solaris operating systems, MySQL, Oracle®, DB2®, or SQL Server database servers, and web environments.

Additional information

The resources in this table can help you learn more about LiveCycle ES.

For information about	See
Preparing to Upgrade to LiveCycle ES	*Preparing to Upgrade to LiveCycle ES* at http://www.adobe.com/go/learn_lc_upgradePreparation
Performing administrative tasks for LiveCycle ES	*Administering LiveCycle ES* at http://www.adobe.com/go/learn_lc_administration
Installing LiveCycle Workbench ES	*Installing Your Development Environment* at http://www.adobe.com/go/learn_lc_installWorkbench
Other services and products that integrate with LiveCycle ES	www.adobe.com
Patch updates, technical notes, and additional information on this product version	www.adobe.com/go/learn_lc_support http://www.adobe.com/cfusion/knowledgebase/index.cfm

Conventions used in this guide

This guide uses the following naming conventions for common file paths.

Name	Default value	Description
[LiveCycleES root]	Windows: C:\Adobe\LiveCycle8\ Linux and UNIX: /opt/adobe/livecycle8/	The installation directory that is used for all LiveCycle ES solution components. The installation directory contains subdirectories for LiveCycle Configuration Manager, the LiveCycle ES SDK, and each LiveCycle ES solution component installed (along with the product documentation). This directory also includes directories relating to third-party technologies.
[LiveCycle7 root]	Windows: C:\Adobe\LiveCycle\ Linux and UNIX: /opt/adobe/livecycle/	The installation directory that is used for all LiveCycle 7.x products. The installation directory contains subdirectories for Adobe LiveCycle Configuration Manager, product SDKs, and each LiveCycle product installed (along with the product documentation).

Name	Default value	Description
[appserver root]	WebSphere on Windows: C:\IBM\WebSphere\AppServer WebSphere on Linux and Solaris: /opt/IBM/WebSphere/AppServer WebSphere on AIX: /usr/IBM/WebSphere/AppServer	The home directory of the application server that runs the LiveCycle ES services.
[dbserver root]	Depends on the database type and your specification during installation.	The location where the LiveCycle ES database server is installed.

Most of the information about directory locations in this guide is cross-platform (all file names and paths are case-sensitive on Linux and UNIX). Any platform-specific information is indicated as required.

1 Introduction

Upgrading to LiveCycle ES from LiveCycle 7.x requires you to install the LiveCycle ES files to your hard disk, and then configure, upgrade, and deploy LiveCycle ES to your application server using the LiveCycle Configuration Manager tool.

This section provides information to help you understand the LiveCycle ES upgrade process, including how it fits in with the installing, configuring, and deploying process.

For information about preparing your system for installing and upgrading to LiveCycle ES, see *Preparing to Upgrade to LiveCycle ES* at http://www.adobe.com/go/learn_lc_upgradePreparation. This document includes information about system requirements, compatibility, API changes, and other information you need to understand before you begin upgrading your LiveCycle 7.x environment.

Note: You do not need to refer to the *Installing and Deploying LiveCycle ES* documents if you are upgrading to LiveCycle ES. This document, combined with *Preparing to Upgrade to LiveCycle ES* at http://www.adobe.com/go/learn_lc_upgradePreparation, contains all the information you need to upgrade LiveCycle 7.x to LiveCycle ES.

About installing, configuring, and deploying LiveCycle ES

Most of the work involved in upgrading from LiveCycle 7.x to LiveCycle ES is done by LiveCycle Configuration Manager. The tasks specific to upgrading are integrated seamlessly into the configuration and deployment process.

Installing, configuring, and deploying LiveCycle ES involves the following processes:

Installing: You install LiveCycle ES by running the installation program. Installing LiveCycle ES places all of the required files onto your computer, within one installation directory structure. The default installation directory is C:\Adobe\LiveCycle8 (Windows) or /opt/adobe/LiveCycle8 (Linux or UNIX); however, you can install the files to a different directory. In this guide, the default installation directory is referred to as *[LiveCycleES root]*. (See "Installing the Solution Component Files" on page 15.)

Configuring and assembling: Configuring LiveCycle ES modifies a variety of settings that determine how LiveCycle ES works. Assembling the product places all of the installed components into several deployable EAR and JAR files according to your configuration instructions. You configure and assemble the components for deployment by running LiveCycle Configuration Manager. (See "Configuring LiveCycle ES for Deployment" on page 42.) You can configure and assemble multiple LiveCycle ES solution components at the same time.

Configuring the application server: You can choose to let LiveCycle Configuration Manager configure the application server for you. Although you already performed some configuration tasks when you prepared the environment for upgrading, there are few more things to do after LiveCycle ES is installed, such as configuring Java Virtual Machine (JVM) arguments, configuring the data source connections, and setting some time-out values. You can choose to perform these tasks manually; the instructions are provided in this document. (See "Configuring LiveCycle ES for Deployment" on page 42.)

Deploying: Deploying the product involves deploying the assembled EAR files and supporting files to the WebSphere application server on which you plan to run your LiveCycle ES solution. If you have configured and assembled multiple solution components, the deployable components are packaged within the deployable EAR files. Components and LiveCycle ES archive files (LCAs) are packaged as JAR files. LiveCycle Configuration Manager automatically deploys the components and archive files to the application server.

Initializing the LiveCycle ES database: Initializing the database creates tables for use with User Management and other solution components. LiveCycle Configuration Manager initializes the LiveCycle ES database after the deployment process. (See "Determining the application server SOAP port" on page 43.)

About upgrading

When you choose the upgrade option in LiveCycle Configuration Manager, LiveCycle Configuration Manager performs upgrading tasks such as extracting data from the LiveCycle 7.x EAR files and importing it into the LiveCycle ES configuration and database, migrating essential data from the LiveCycle 7.x configuration, unlocking and migrating security credentials. You are prompted to provide information about your LiveCycle 7.x system as you proceed.

How the LiveCycle upgrade works

Upgrading to LiveCycle ES from products of any version of LiveCycle 7 involves these tasks:

1. Upgrading the application server and database (new versions are supported in LiveCycle ES). Instructions for this task are described in *Preparing to Upgrade to LiveCycle ES* at http://www.adobe.com/go/learn_lc_upgradePreparation.
2. Installing LiveCycle ES product files.
3. Running LiveCycle Configuration Manager to initiate the configuration, upgrading, and deployment process. The next four steps (below) are included in this process.
4. Extracting configuration settings and data from LiveCycle 7.x EAR files and applying them to the LiveCycle ES EAR files and database. (Not applicable to LiveCycle Policy Server upgrades.)
5. Applying a compatibility layer to the LiveCycle ES EAR files. The compatibility layer comprises a set of deprecated Enterprise JavaBeans™ (EJBs), classes, servlets, and CORBA APIs, which support custom applications developed with LiveCycle 7.x and enable these legacy applications to continue to work with LiveCycle ES. (Not applicable to LiveCycle Policy Server upgrades.)
6. Starting LiveCycle ES on the application server so that it is available to accept user requests.
7. Migrating data to the LiveCycle ES database for LiveCycle 7.x products that used User Management or a database to store other data (LiveCycle Workflow, LiveCycle Form Manager, LiveCycle Forms, and LiveCycle PDF Generator).
8. Migrating LiveCycle Policy Server data to the LiveCycle ES database.
9. Migrating remaining data, such as audit records for LiveCycle Policy Server, submitted or historical data associated with LiveCycle Workflow.

Post-deployment upgrade tasks

Some manual steps are required after you complete the upgrade and deployment process to ensure that LiveCycle 7.x properties have been fully migrated to LiveCycle ES and that LiveCycle 7.x client applications can be run in LiveCycle ES. (See "Post-Deployment Activities" on page 53.)

Updating client applications

Client applications developed using LiveCycle 7.x may need to be updated with new client JAR files in the following circumstances:

- LiveCycle 7.x client applications running on WebSphere use the um-client.jar file or are stand-alone and running on Java 1.4
- LiveCycle Forms version pre-7.2 client applications on WebSphere
- LiveCycle 7.x client applications are written for LiveCycle Forms 7.0 or 7.1 (pre-7.2) running on WebSphere.

Client applications using um-client.jar

The LiveCycle 7.x version of the um-client.jar file is not compatible with LiveCycle ES running on WebSphere. If any LiveCycle 7.x client applications use this file, they must be updated to use the LiveCycle ES adobe-usermanager-client.jar file instead of the um-client.jar file from LiveCycle 7.x. After LiveCycle ES is installed, the new um-client.jar file is in the *[LiveCycleES root]*/LiveCycle_ES_SDK/client-libs/common directory.

Client applications that will continue to run on Java 1.4

All client applications ran on Java 1.4 in LiveCycle 7.x. If stand-alone LiveCycle 7.x applications (applications running remotely from the LiveCycle server) will be moved to run on Java 5 when you upgrade to LiveCycle ES, the WebSphere 5.1.x or WebSphere 6.0.x client JAR files must be replaced with WebSphere 6.1 client JAR files.

If the LiveCycle 7.x client application will continue to run on Java 1.4 after upgrading to LiveCycle ES, this update is not required.

LiveCycle Forms version pre-7.2 client applications

LiveCycle Forms client applications that were developed using a version of LiveCycle Forms earlier than version 7.2 (for example, 7.0 or 7.1) running on WebSphere require the replacement of five LiveCycle Forms 7.2 JAR files.

The LiveCycle Forms 7.2 JAR files are included in the LiveCycle ES installation in the following locations in the *[LiveCycle ES root]/*LiveCycle_ES_SDK/client-libs/upgrade/lc72/components/ directory:

- /csa/common/lib/adobe/adobe-common.jar
- /csa/common/lib/adobe/datamanager-client.jar
- /csa/websphere/lib/adobe/AdobeCSAUtils.jar
- /csa/websphere/lib/adobe/DocumentServiceLibrary.jar
- /forms/common/lib/adobe/formserver-client.jar

It is recommended that you update the client applications to point to these JAR files.

Updating LiveCycle QPACs

LiveCycle ES supports LiveCycle 7.x workflows, which can continue to operate without modification. However, to take advantage of new features that LiveCycle ES services provide, you can upgrade workflows so that QPAC-based actions are replaced with equivalent LiveCycle ES service operations.

It is necessary to eventually migrate all processes that use LiveCycle 7.x QPACs to use new LiveCycle ES components to ensure that processes remain compatible with future releases of LiveCycle ES. The Process Upgrade Tool is part of Workbench ES, and you can use it at any time to upgrade a LiveCycle 7.x QPAC to a LiveCycle ES service component. Only Adobe-provided QPACs can be upgraded using the Process Upgrade Tool.

You can upgrade custom QPACs by creating an upgrade definition file that is used by the Process Upgrade Tool. The upgrade definition file describes how the customer QPAC created in LiveCycle 7.x maps to a LiveCycle ES service component.

Upgrading LiveCycle Barcoded Forms QPACs is not supported by Process Upgrade Tool.

LiveCycle Policy Server QPACs will be supported in a future release of LiveCycle ES.

Note: When a LiveCycle 7.x workflow that generates CSS2HTML is upgraded to a LiveCycle ES process using the Process Upgrade Tool in Workbench ES, the upgraded process outputs XHTML instead of CSS2HTML.

Selecting tasks for configuring and deploying LiveCycle ES

After you install LiveCycle ES, you can run LiveCycle Configuration Manager to perform a variety of tasks. The first task you choose is to upgrade from LiveCycle 7.x to LiveCycle ES. Then you can select the following tasks for LiveCycle Configuration Manager to perform, in addition to the upgrade:

- Configure LiveCycle ES solution components in an EAR file for deploying to the application server.
- Configure application server properties to support LiveCycle ES
- Validate application server configuration
- Deploy LiveCycle ES EAR files
- Initialize the LiveCycle ES database
- Deploy LiveCycle ES components
- Validate the LiveCycle ES component deployment
- Configure the LiveCycle Reader Extensions ES Rights credential (if Reader Extensions ES is installed)
- Initialize BAM metadata for LiveCycle Business Activity Monitoring ES (if Business Activity Monitoring ES is installed)
- (Optional) Import the LiveCycle ES Samples

Although you can use LiveCycle Configuration Manager to configure the application server to set up data sources and JVM arguments, you may prefer to complete these steps manually. For information about the tasks involved in this installation method, see "Manual installation and deployment checklist" on page 13.

Installation, configuration, upgrading, and deployment checklists

This section includes checklists that you can use to step through the installation, configuration, and upgrade process. A checklist is provided for installing, configuring, and upgrading when using either the automatic method or the manual method.

The *automatic method* refers to using LiveCycle Configuration Manager to configure LiveCycle ES, configure the application server, and deploy the solution components to the server.

The *manual method* refers to using LiveCycle Configuration Manager to configure and deploy LiveCycle ES and initialize (bootstrap) the database; however, configuring the application server and configuring database connectivity is done manually by the administrator by using the instructions later in this guide.

Automatic installation and deployment checklist

The following table includes the steps required for installing LiveCycle ES solution components using the automatic method. WebSphere must be installed before you perform the installation.

Task	Topic
Ensure that you have the required software installed in the target environment. This should include installing the new application server and databases required for the LiveCycle ES deployment.	*Preparing to Upgrade to LiveCycle ES* at http://www.adobe.com/go/learn_lc_upgradePreparation
Run the installation program to install LiveCycle ES on your system.	"Installing the Solution Component Files" on page 15
Run LiveCycle Configuration Manager and select Upgrade from LiveCycle 7.x, and then select the products you are upgrading from. You will also select corresponding LiveCycle ES solution components that you are upgrading to or configuring for the first time.	"Configuring LiveCycle ES for Deployment" on page 42
Select all the tasks on the Task Selection screen. This will configure and assemble the LiveCycle ES EAR files, configure application server settings, deploy the EAR files and other components to the application server, initialize the LiveCycle ES database, and verify the deployment. Various upgrade-specific tasks are included.	"Configuring LiveCycle ES for Deployment" on page 42
Access LiveCycle Administration Console and User Management.	"Accessing LiveCycle Administration Console" on page 53

Task	Topic
Configure LDAP access.	"Configuring LiveCycle ES to access LDAP" on page 60
Complete post-deployment upgrade tasks, including repackaging LiveCycle 7.x client applications to include the LiveCycle ES client JAR files.	"Post-Deployment Activities" on page 53

Manual installation and deployment checklist

The following table includes the steps required for installing LiveCycle ES using the manual method.

Task	Topic
Ensure that you have the required software installed and configured in the target environment.	*Preparing to Upgrade to LiveCycle ES* at http://www.adobe.com/go/learn_lc_upgradePreparation
Ensure that files, directories, and databases associated with LiveCycle 7.x are fully backed up.	*Preparing to Upgrade to LiveCycle ES* at http://www.adobe.com/go/learn_lc_upgradePreparation
(LiveCycle PDF Generator upgrade only) Install Adobe Acrobat® 8.1 from the LiveCycle ES media.	"Installing Acrobat for LiveCycle PDF Generator ES" on page 15.
Run the installation program.	"Installing the Solution Component Files" on page 15
Configure WebSphere settings. A variety of settings must be configured.	"Manually Configuring WebSphere" on page 21
Run LiveCycle Configuration Manager and select Upgrade from LiveCycle 7.x, and then select the products you are upgrading from. You will also select corresponding LiveCycle ES solution components that you are upgrading to or configuring for the first time.	"Configuring LiveCycle ES for Deployment" on page 42
In LiveCycle Configuration Manager, select all the tasks except Configure Application Server, Validate Application Server Configuration, and Deploy LiveCycle ES EARs (these appear dimmed on the Task Selection screen). This will configure and assemble the LiveCycle ES EAR files, deploy the supporting components to the application server, initialize the LiveCycle ES database, and verify the deployment. Various upgrade-specific tasks are included.	"Configuring LiveCycle ES for Deployment" on page 42

Task	Topic
If the application server targeted for LiveCycle ES is installed on the same computer as the LiveCycle 7.x application server, configure the LiveCycle ES application server when LiveCycle Configuration Manager prompts you to stop the LiveCycle 7.x server.	"Configuring LiveCycle ES for Deployment" on page 42
Return to LiveCycle Configuration Manager to complete the upgrade and migration process, component deployment, and initialization of LiveCycle ES.	"Configuring LiveCycle ES for Deployment" on page 42
Access LiveCycle Administration Console and User Management.	"Accessing LiveCycle Administration Console" on page 53
Configure LDAP access. (LiveCycle Policy Server upgrade migrates LDAP settings automatically.)	"Configuring LiveCycle ES to access LDAP" on page 60
Update LiveCycle 7.x client applications as necessary.	"Updating client applications" on page 10

2 Installing the Solution Component Files

This section describes the first phase of setting up a LiveCycle ES system that is running the LiveCycle installation program on a Windows, Linux, or UNIX operating system. A subsequent phase will include running LiveCycle Configuration Manager to configure, upgrade, and deploy LiveCycle ES.

Before you install the solution components, you must ensure that your environment includes the software and hardware required to run LiveCycle ES. You should also understand the installation options and have prepared the environment as required. (See *Preparing to Upgrade to LiveCycle ES* at http://www.adobe.com/go/learn_lc_upgradePreparation.)

Note: If you are upgrading any products that use LiveCycle 7.x QPACs (called *components* in LiveCycle ES), you must upgrade LiveCycle Workflow 7.x to LiveCycle Process Management ES. If Process Management ES is not included in the LiveCycle ES deployment, QPACs cannot be used.

Installing Acrobat for LiveCycle PDF Generator ES

Note: This section applies only if your configuration requires native file format conversion (for example, Microsoft Word to PDF).

LiveCycle PDF Generator ES can convert many native file formats to PDF. Such native file formats include Microsoft Word, Microsoft Excel, Microsoft PowerPoint, Microsoft Project, Microsoft Visio, Corel WordPerfect, Adobe Photoshop®, Adobe FrameMaker®, and Adobe PageMaker®. For more information about PDF Generator ES, see the *LiveCycle ES Overview* at http://www.adobe.com/go/learn_lc_overview

If you plan to use PDF Generator ES native application format conversion or optical character recognition (OCR) generation, you must install Acrobat 8.1 on the computer where PDF Generator ES will run before you run the LiveCycle ES installation program. If you do not install Acrobat 8.1 prior to installing LiveCycle ES, you must install Acrobat 8.1 afterward and perform some additional manual tasks. A copy of Acrobat 8.1 is included on the LiveCycle ES DVD.

If you do not want to configure PDF Generator ES to support this functionality, you do not need to install or upgrade to Acrobat 8.1. However, it is recommended that you upgrade to Acrobat 8.1 in order to support conversions using Microsoft Office 2007.

➤ **To install Acrobat 8.1 for PDF Generator ES:**

1. Uninstall any other version of Acrobat by using the **Add/Remove Programs** window in the Windows Control Panel.
2. Restart your computer if prompted.
3. Navigate to one of the following folders on the LiveCycle ES installation media, depending on your locale:
   - additional\acrobat\efg\Adobe Acrobat 8 Professional
   - additional\acrobat\jpn\Adobe Acrobat 8 Professional
4. Double-click the **Setup.exe** file to run the Acrobat installer.
5. Follow the instructions on the Acrobat installer screens.

Installing LiveCycle ES

You can install LiveCycle ES on the same computer as the application server where it will be deployed or on a separate computer. However, the computer on which the LiveCycle ES files are installed must have file network access to the LiveCycle 7.x EAR files, the Global document storage directory, the target application server, and the LiveCycle 7.x and LiveCycle ES databases. For more information, see "Installation and deployment topology considerations" in *Preparing to Upgrade to LiveCycle ES* at http://www.adobe.com/go/learn_lc_upgradePreparation.

After you install LiveCycle ES, you will run LiveCycle Configuration Manager to perform the upgrade from LiveCycle 7.x to LiveCycle ES. If the LiveCycle ES server is on a separate computer from the LiveCycle 7.x computer and you want to configure the application server manually rather than have LiveCycle Configuration Manager do the task, you can do it before you run LiveCycle Configuration Manager to perform the upgrade.

To successfully install LiveCycle ES, you need read and write permissions for the installation directory. The following installation directories are the defaults; however, you can specify a different directory as required:

- (Windows) C:\Adobe\LiveCycle8\
- (Linux and UNIX) /opt/adobe/livecycle8/

When installing on Linux, the installation program uses the logged-in user's home directory as a temporary directory for storing files. As a result, messages such as this one may appear in the console:

```
WARNING: could not delete temporary file /home/<username>/ismp001/1556006
```

When you complete the installation, you must manually delete the temporary files.

Caution: Ensure that the temporary directory for your operating system meets the minimum requirements as outlined in *Preparing to Upgrade to LiveCycle ES* at http://www.adobe.com/go/learn_lc_upgradePreparation. The temporary directory is one of the following locations:

- (Windows) TMP or TEMP path as set in the environment variables
- (Linux) Logged-in user's home directory
- (Solaris) /var/tmp
- (AIX) /tmp

Note: When you are installing the solution component on a Linux or UNIX operating system, you must be logged in as the root user to successfully install the solution component to the default location /opt/adobe/LiveCycle8/. If you are logged in as a non-root user, you must change the installation directory to one for which you have permissions (for example, $HOME/adobe/LiveCycle8).

Installing to a Windows staging platform for deployment on Linux or UNIX

LiveCycle ES can be installed and configured on Windows for deployment on a Linux or UNIX platform. You can use this functionality for locked-down Linux environment. For example, a locked-down environment would not have Windows installed. When you run the installation program on Windows, you can choose a Linux or UNIX operating system as the target platform for deploying LiveCycle ES. The installation program installs binaries for Linux, or Solaris, which are also used by LiveCycle Configuration Manager when you configure the product.

The computer running Windows can then be used as a staging location for the deployable objects, which can be copied to a Linux or UNIX computer for deployment to the application server. The application server that you are targeting must be consistent with what you choose during installation and configuration regardless of the operating system.

Note: The host and target operating system must be Windows to support installing Acrobat for PDF Generator ES from the installer.

Configuring the LiveCycle Reader Extensions ES Rights credential

If you are upgrading LiveCycle Reader Extensions 7.x to LiveCycle Reader Extensions ES, ensure that you have a new valid credential and password before running the installation. If you do not have this information at this time, you can install the credential after you install and deploy LiveCycle ES on the Trust Store configuration pages in the LiveCycle Administration Console. You must use the name of your LiveCycle 7.x Rights credential for LiveCycle ES. If you use a different name, you will have to modify code in existing custom applications or, in future LiveCycle ES, your existing LiveCycle QPACs.

Including the Java 5 SDK in the JAVA_HOME environment variable

The `JAVA_HOME` environment variable must point to the Java 5 SDK. The required Java SDK is IBM JDK 1.5.0 SR3 (embedded in application server) on all platforms except Solaris. On Solaris, you must point to Sun JDK 1.5.0_09.

The Java 5 SDK requirements are also listed in *Preparing to Upgrade to LiveCycle ES* at http://www.adobe.com/go/learn_lc_upgradePreparation.

➤ **To install LiveCycle ES:**

1. Navigate to the /livecycle_server/8.0 directory of the installation media.
2. Start the installation program:
   - (Windows) Double-click the win_livecycle8_setup.exe file.
   - (Linux, UNIX) From a command prompt, type the file name appropriate for your operating system:

     ```
     ./aix_livecycle8_setup.bin
     ./linux_livecycle8_setup.bin
     ./solaris_livecycle8_setup.bin
     ```

   Note: If you are installing to a Windows staging platform for deployment to Linux or UNIX, start the Windows executable.
3. On the Welcome screen, click **Next**.
4. On the Destination screen, accept the default directory as listed or click **Browse** and navigate to the directory where you want to install the solution component, and then click **Next**.

   Note: If you type the name of a directory that does not exist, it will be created for you.

Caution: When you install the solution component, you can specify a different installation location. If you are installing on Linux, or UNIX, the directory you specify should not contain any spaces; otherwise, the installation program does not install the solution component.

5. Type a serial number for the LiveCycle ES solution components in the text box and click **Add**. If you have licensed multiple solution components, repeat this step for each serial number you have. When you have added all the serial numbers to the list, click **Next**.

Tip: To reset the serial number, click **Clear**.

6. Read the Product License Agreement and, if you agree, select **I accept the terms of the license agreement**, and then click **Next**. Otherwise, you cannot proceed with the installation.

7. (Windows only) Select the operating system for which you plan to configure LiveCycle ES, and click **Next.**

   Note: At this point, you can specify to use Windows as a staging platform for your deployment. You can select a Linux or UNIX operating system as the target for deployment even if you installing on Windows.

8. ***(PDF Generator ES only)*** Select the appropriate option on the PDF Generator ES screen:

   Yes, enable native application support for LiveCycle PDF Generator ES: Select this option to have the software check the version of Acrobat you have installed. If you do not have Acrobat installed, accept the prompt to install Acrobat 8.1 now.

   If you have an unsupported version of Acrobat installed (earlier than Acrobat 8.0), complete the LiveCycle ES installation, uninstall Acrobat, and then install Acrobat 8.1 from the LiveCycle ES DVD by following the instructions in the procedure "To configure Acrobat 8.1 for use with PDF Generator ES:" on page 19. If you have Acrobat 8.0 installed, you can upgrade to LiveCycle 8.1.

   No, do not enable native application support for LiveCycle PDF Generator ES: Select this option if you are installing in a clustered environment, and then go to step 9.

9. Review the installation details and then click **Install**. The installation program displays the progress of the installation. A summary screen appears when the solution component installation is completed.

10. Review the release notes that are displayed and click **Next**.

11. Deselect **Start LiveCycle Configuration Manager.**

12. Click **Finish** and go to "Specifying class path and JAVA_HOME" on page 19.

Caution: If you are upgrading a platform that includes an Oracle database, do not select **Start LiveCycle Configuration Manager**. Instead, start LiveCycle Configuration Manager using the startup script according to the instructions in the section "Configuring LiveCycle ES for Deployment" on page 42.

Note: Selecting the Start option starts LiveCycle Configuration Manager, which allows you to complete your configuration and deployment immediately. If you are not ready to run LiveCycle Configuration Manager immediately, ensure that the Start LiveCycle Configuration Manager option is not selected when you click **Finish**. You can start LiveCycle Configuration Manager at a later time.

When you are ready to proceed with the configuration and deployment, see "Configuring LiveCycle ES for Deployment" on page 42.

➤ **To configure Acrobat 8.1 for use with PDF Generator ES:**

This procedure is required only if you upgraded to or installed Acrobat 8.1 after completing the LiveCycle ES installation. It can be completed before or after you run LiveCycle Configuration Manager and deploy LiveCycle ES to the application server.

1. If an unsupported version of Acrobat (earlier than 8.0) is installed, uninstall it by using the Add or Remove Programs window in the Windows Control Panel.
2. Install Acrobat 8.1 from the LiveCycle ES DVD by running the Setup.exe file from the /additional/acrobat directory.
3. When the installation is complete, open a Windows command prompt and navigate to the /additional/scripts directory on the LiveCycle ES installation media.
4. Run the following command:

```
Acrobat_for_PDFG_Configuration.bat [LiveCycleES root]
```

➤ **To validate the Acrobat 8.1 installation:**

- Navigate to a PDF file on your system and double-click it to open it in Acrobat.

  If the PDF file opens successfully, Acrobat 8.1 is installed correctly. If the PDF fails to open correctly, uninstall Acrobat and reinstall it.

Viewing the error log

If any errors occur during the installation, the installation program creates a log file called *log.txt*, which contains the error messages. The log file is located in the *[LiveCycleES root]* directory.

For information about errors that may occur during installation, see "Troubleshooting" on page 70.

Specifying class path and JAVA_HOME

If you are upgrading to LiveCycle ES from LiveCycle 7.x, you must specify the class path and `JAVA_HOME` environment variable before you start LiveCycle Configuration Manager. The `JAVA_HOME` environment variable must point to the Java 5 SDK. The required Java SDK is IBM JDK 1.5.0 SR3 (embedded in application server) on all platforms except Solaris. On Solaris, you must point to Sun JDK 1.5.0_09.

➤ **To set the class path and JAVA_HOME on Windows:**

1. Open a command window, and clear the `PATH` environment variable by typing the following command:

```
set PATH=
```

2. Set up the WebSphere command-line environment by typing the following commands:

```
cd [appserver root]
.\bin\setupCmdLine.bat
```

3. Start LiveCycle Configuration Manager by typing the following commands:

```
cd [LiveCycle_ES_ROOT]/configurationManager/bin
ConfigurationManager.bat
```

➤ **To set the class path and JAVA_HOME on Linux and UNIX:**

1. Open a command window, and clear the `PATH` environment variable by typing the following command:

   ```
   export PATH=
   ```

2. Set up the WebSphere command-line environment by typing the following commands:

   ```
   cd [appserver root]
   ./bin/setupCmdLine.bat
   ```

3. Start LiveCycle Configuration Manager by typing the following commands

   ```
   cd [LiveCycleES root]/configurationManager/bin
   ConfigurationManager.sh
   ```

Next steps

You must now configure and upgrade LiveCycle ES for deployment. (See "Configuring LiveCycle ES for Deployment" on page 42.)

3 Manually Configuring WebSphere

This chapter describes how to manually configure the application server to prepare for the manual deployment of LiveCycle ES in a non-clustered environment. If you prefer to have LiveCycle Configuration Manager configure WebSphere, you do not need to complete this chapter; instead, go to "Configuring LiveCycle ES for Deployment" on page 42.

The time at which you perform the tasks in this section depends on whether the target application server for LiveCycle ES is installed on the same computer as the LiveCycle 7.x server or a different computer:

Target application server for LiveCycle ES is on the *same* computer as LiveCycle 7.x server

Do not perform these tasks until you are partway through the LiveCycle ES upgrade using LiveCycle Configuration Manager. When you are prompted by LiveCycle Configuration Manager and the documentation to stop LiveCycle 7.x, you can do so, and then start the application server for LiveCycle ES and configure it. In this case, you must first complete the tasks in the "Configuring WebSphere Application Server" section of *Preparing to Upgrade to LiveCycle ES* (at http://www.adobe.com/go/learn_lc_upgradePreparation.

and then complete the tasks in this section.

Note: Because the LiveCycle 7.x server and LiveCycle ES target application server cannot be started at the same time on the same computer, performing the tasks in this order minimizes server down time.

Target application server for LiveCycle ES is on a *different* computer than LiveCycle 7.x server

You can configure the LiveCycle ES application server after you install LiveCycle ES but before you run LiveCycle Configuration Manager. (This order of tasks is reflected in the order of the sections in this document.)

Note: You must have configured your WebSphere Application Server according to the instructions in the "Configuring WebSphere Application Server" chapter of *Preparing to Upgrade to LiveCycle ES*.

Configuring the JVM arguments and properties

You must configure the JVM arguments and custom properties.

➤ **To configure the JVM arguments:**

1. In the URL line of a web browser, type the appropriate URL:

   `http://[host name]:[port]/ibm/console`

   If you are administering the server you are currently using, you can replace `[hostname]` with `localhost`. The port value will depend on the application server and whether Global Security is enabled. The default port value for WebSphere 6.1.0.5 is 9060. If Global Security is enabled, the default SSL port value is 9043.

2. If WebSphere Global Security is enabled, type the WebSphere user ID and password in the boxes provided.

3. Click **Log In**.

4. In the WebSphere Administrative Console navigation tree, click **Servers** > **Application Servers** and, in the right pane, click the server name.
5. Under Server Infrastructure, click **Java and Process Management** > **Process Definition**.
6. Under Additional Properties, click **Java Virtual Machine**.
7. In the **Initial Heap Size** box, type `256` and, in the **Maximum Heap Size** box, type `1024`.

Note: This value depends on the hardware configuration and the available memory. Setting this value to zero (0) might be preferable because it means NOMAX. Setting the value to zero does not mean that the heap grows infinitely large because the initial heap size parameter ensures that the garbage collector runs periodically to limit heap growth.

8. In the **Generic JVM arguments** box, type `-Dfile.encoding=utf8` and then click **OK**.
9. Under Additional Properties, click **Custom Properties**, and then click **New**.
10. In the **Name** box, type `java.net.preferIPv4Stack` and, in the **Value** box, type `true`.
11. Click **OK** or **Apply**.
12. In the **Messages** box, click **Save directly to master configuration**.

You need to create a J2C Authentication to assign to your data source.

➤ **To create a J2C authentication configuration for the data source:**

1. In the navigation tree, click **Security** > **Secure administration, applications, and infrastructure**.
2. In the right pane, under Authentication, click **Java Authentication and Authorization Service** > **J2C authentication data**.
3. Click **New**.
4. Provide the required information in these boxes:

   Alias: Type a name appropriate for the database user (for example, type `IDP_DS/db2-db2user`).

   User ID: Enter a user ID. This ID is the login credential used to access the database that will be used with the IDP_DS data source (for example, db2user).

   Password: Type a password for this user.
5. Click **OK** or **Apply**.
6. Click **Save directly to master configuration**.

Configuring WebSphere time-out settings

Creation of a large number of users can be done by using a single invocation of the CreateLocalUsers API. The API is expected to persist all the new users or roll back all changes in the event of a failure. Therefore, the API is required to operate in a single transaction to support rollback. Because a transaction's lifetime is limited by the application server settings (usually 30 seconds), the number of inserts that can be performed in the given time frame is limited. As a result, bulk insert APIs, such as CreateLocalUser, fail when the number of users exceeds a certain limit. This limit is decided again by the transaction's lifetime.

You must modify the following time-out settings:

- Transaction time-out value
- CORBA time-out value

➤ **To configure transaction time-out:**

1. In the WebSphere Administrative Console navigation tree, click **Servers** > **Application servers** and, In the right pane, click the server name.
2. Under Container Settings, click **Container Services** > **Transaction Service**.
3. Under General Properties, in the **Total transaction lifetime timeout** box, type `300` (or higher).
4. Ensure that the value in the **Maximum transaction timeout** box is greater than or equal to the total transaction time-out.
5. Click **OK** or **Apply**.

➤ **To increase the CORBA time-out value:**

1. In the navigation tree, click **Servers** > **Application servers** and, in the right pane, click the server name.
2. Under Container Settings, click **Container Services** > **ORB Service**.
3. Under General Properties, in the **Request timeout** box, type `360` and, in the **Locate Request Timeout** box, type `300`.
4. Click **OK** or **Apply**.
5. In the **Messages** box, click **Save directly to master configuration**.

Increasing transaction time-out and ORB service values for PDF Generator ES

If you installed and deploy PDF Generator ES, you must increase the maximum transaction time-out and ORB service values on WebSphere to ensure that document conversions by PDF Generator ES complete successfully.

You can increase the transaction time-out and ORB service value before or after you deploy PDF Generator ES.

➤ **To increase the maximum transaction time-out and ORB service values:**

1. In the WebSphere Administrative Console navigation tree, click **Servers** > **Application Servers** and, in in the right pane, click the server name.
2. Under Container Settings, click **Container Services** > **Transaction Service**.
3. In the **Maximum transaction timeout** box, type `300` (or higher) and, in the **Total transaction lifetime timeout** box, change 120 to 300.
4. Click **OK** or **Apply**.
5. In the **Messages** box, click **Save directly to master configuration**.

Configuring throttling for LiveCycle PDF Generator ES

PDF Generator ES requires a throttling configuration to be added to the application server configuration.

➤ **To set the PDF Generator ES throttling configuration:**

1. In the WebSphere Administrative Console navigation tree, click **Servers** > **Application Servers** and, in in the right pane, click the server name.
2. Under Server Infrastructure, click **Java and Process Management** > **Process Definition**.
3. Under Additional Properties, click **Java Virtual Machine** and, on the next screen, click **Custom Properties**.
4. Click **New** and, in the following boxes, type the corresponding text to create a new property:

   Name: `com.ibm.websphere.ejbcontainer.poolSize`

   Value: `LiveCycle8#adobe-pdfg-bmc-invoker-ejb.jar#NativeToPDFInvoker=1,1:LiveCycle8#adobe-pdfg-bmc-invoker-ejb.jar#OpenOfficeToPDFInvoker=1,1:LiveCycle8#adobe-pdfg-bmc-invoker-ejb.jar#ImageToPDFInvoker=3,3:LiveCycle8#adobe-pdfg-bmc-invoker-ejb.jar#PSToPDFInvoker=3,3`

   Note: You must manually type the value. You cannot copy and paste the value from this document.

   In the example, `LiveCycle8` is the name of the LiveCycle ES 8.0 core application as shown in the WebSphere Application Server. If this name is different, all four instances of the string `LiveCycle8` in the value parameter must be replaced with the actual application name.

   Description: `Adobe PDF Generator Throttling Configuration`
5. Click **OK** or **Apply**.
6. In the **Messages** box, click **Save directly to master configuration**.

Configuring the LiveCycle ES database connectivity

To enable WebSphere and your LiveCycle ES deployment to connect to the LiveCycle ES database, you must create a database connection for LiveCycle ES by installing the database drivers and then setting up a data source.

You must install drivers for the type of database that you use for the LiveCycle ES database. The drivers must be placed in the installation directories of the application server.

You must configure the data source to connect to the database. For WebSphere, you can configure a DB2, an Oracle 10g, or a SQL Server 2005 data source.

You will need the following information from tasks you did in *Preparing to Install LiveCycle ES*, which is available at http://www.adobe.com/go/learn_lc_prepareInstall:

- Database name
- Server name
- User name
- Password

Configuring the DB2 data source

Configuring the DB2 data source requires you to install the DB2 database drivers, create a DB2 JDBC provider on WebSphere, create the data source on WebSphere, and then configure the corresponding connection pool.

➤ **To install the DB2 database driver:**

1. In the *[appserver root]* directory, create a directory named *db2libs*.
2. Copy the db2jcc_license_cu.jar and db2jcc.jar files from one of these locations to the *[appserver root]*\db2libs directory:
   - The java directory under your *[dbserver root]* directory, such as *[dbserver root]*/ibm/Sqllib/java (Windows) or *[dbserver root]*/java (Linux or UNIX)
   - *[LiveCycleES root]*\lib\db\db2

➤ **To create a DB2 JDBC provider:**

1. In the WebSphere Administrative Console navigation tree, click **Environment** > **Websphere Variables** and, in the right pane, click **DB2UNIVERSAL_JDBC_DRIVER_PATH**.
2. In the **Value** box, type the path to the db2libs directory.
3. Click **OK** or **Apply**.
4. Click **Save directly to master configuration**.
5. In the navigation tree, click **Resources** > **JDBC** > **JDBC Providers**.
6. In the drop-down list in the right pane, select **Node** (without server) as the level, and then click **New**.
7. In the Step 1 pane, set the following configuration:
   - In the **Database type** list, select **DB2**.
   - In the **Provider type** list, select **DB2 Universal JDBC Driver Provider**.
   - In the **Implementation type** list, select **Connection pool data source**. Take note that for each LiveCycle Configuration Manager configuration script, the field implementation class name is com.ibm.db2.jcc.DB2ConnectionPoolDataSource.
   - In the **Name** box, keep the default, which is **DB2 Universal JDBC Driver Provider**, or type `LiveCycle - db2 - IDP_DS`.
8. Click **Next** and, in the Step 2 pane, click **Next** again.
9. In the Step 3 pane, click **Finish**.
10. In the **Messages** box, click **Save directly to master configuration**.

➤ **To create the DB2 JDBC data source:**

1. In the navigation tree, click **Resources** > **JDBC** > **JDBC Providers** and, in the right pane, click the provider you created in "To create a DB2 JDBC provider:" on page 25.
2. Under Additional Properties, click **Data sources** and then click **New**.
3. In the Step 1 pane, set the following configurations and then click **Next**:
   - In both the **Data source name** box and the **JNDI name** box, type `IDP_DS`.
   - In the list under Component-Managed Authentication and XA Recovery Authentication, select the authentication alias created for this data source in "To create a J2C authentication configuration for the data source:" on page 22, and then click **Next**.
4. In the Step 2 pane, type the database name and server name of the database you created in "To create a J2C authentication configuration for the data source:" on page 22.
5. Ensure that **Use this data source in container managed persistence (CMP)** is selected, and then click **Next**.
6. In the Step 3 pane, click **Finish**.
7. In the right pane, click the data source you just created to modify additional parameters and set the following configuration:
   - In the **Container-managed authentication alias** list, select the authentication alias created for this data source in "To create a J2C authentication configuration for the data source:" on page 22.
   - In the **Mapping-configuration alias** list, select DefaultPrincipalMapping.
8. Click **OK** or **Apply**.
9. Click **Save directly to master configuration**.

➤ **To configure IDP_DS connection pools:**

1. In the navigation tree, click **Resources** > **JDBC** > **JDBC Providers** and, in the right pane, click the data source you just created, either **DB2 Universal JDBC Driver Provider** or **LiveCycle - db2 - IDP_DS**, as used as an example in "To create a DB2 JDBC provider:" on page 25.
2. Under Additional Properties, click **Data sources** and then select **IDP_DS**.
3. On the next screen, under Additional Properties, click **Connection Pool Properties** and set the properties as follows:
   - In the **Maximum connections** box, type `100` or higher if required.
   - In the **Minimum connections** box, type `1`.
4. Click **OK** or **Apply**.
5. Click **Save directly to master configuration**.

➤ **To create the DB2 JDBC data source for LiveCycle Rights Management ES:**

Note: This section applies only if you have installed Rights Management ES.

1. In the navigation tree, click **Resources** > **JDBC** > **JDBC Providers** and click the provider you created in "To create a DB2 JDBC provider:" on page 25.
2. Under Additional Properties, click **Data sources** and then click **New**.
3. In the Step 1 pane, set the following configurations and then click **Next**:
   - In the **Data source name** box, type `RM_DS`.
   - In the **JNDI name** box, type `EDC_DS`.
   - In the list under Component-Managed Authentication and XA Recovery Authentication Alias, select the authentication alias created for this data source in "To create a J2C authentication configuration for the data source:" on page 22.
4. In the Step 2 pane, type the database name and server name of the database you created in "To create a J2C authentication configuration for the data source:" on page 22, and then click **Next**.
5. In the Step 3 pane, click **Finish**.
6. Select the data source you just created to modify additional parameters and set the following configuration:
   - In the **Container-managed authentication alias** list, select the authentication alias created for this data source in "To create a J2C authentication configuration for the data source:" on page 22.
   - In the **Mapping-configuration alias** list, select DefaultPrincipalMapping.
7. Click **OK** or **Apply**.
8. Click **Save directly to master configuration**.

➤ **To configure RM_DS connection pools for LiveCycle Rights Management ES:**

Note: This section applies only if you have installed Rights Management ES.

1. In the navigation tree, click **Resources** > **JDBC** > **JDBC Providers** and, in the right pane, click the **DB2 Universal JDBC Driver Provider for RM** data source you just created.
2. Under Additional Properties, click **Data sources** and then select **RM_DS**.
3. On the next screen, under Additional Properties, click **Connection Pool Properties** and set the properties as follows:
   - In the **Maximum connections** box, enter 100 or higher if required.
   - In the **Minimum connections** box, enter 1.
4. Click **OK** or **Apply**.
5. Click **Save directly to master configuration**.

Configuring the Oracle data source

Configuring the Oracle data source requires you to install the Oracle database drivers, create a Oracle JDBC provider on WebSphere, create the data source on WebSphere, and then configure the corresponding connection pool.

➤ **To install the Oracle 10g database driver:**

1. Download the Oracle 10g Release 2 (10.2.0.2 Thin) driver from the following website:

   www.oracle.com/technology/software/tech/java/sqlj_jdbc/htdocs/jdbc_10201.html

2. In the *[appserver root]* directory, create a directory named *db_driver* and copy to this directory the ojdbc14.jar file that you downloaded.

➤ **To create the Oracle JDBC provider:**

1. In the WebSphere Administrative Console navigation tree, click **Environment** > **Websphere Variables** and, in the right pane, click **ORACLE_JDBC_DRIVER_PATH**.
2. Under General Properties, in the **Value** box, type the path to the ojdbc14.jar file you created in "To install the Oracle 10g database driver:" on page 28 and then click **OK**.
3. In the **Messages** box, click **Save directly to master configuration**.
4. In the navigation tree, click **Resources** > **JDBC** > **JDBC Providers**.
5. In the drop-down list in the right pane, select **Node** (without server) as the level, and then click **New**.
6. In the Step 1 pane, set the following configuration:
   - In the **Database type** list, select **Oracle**.
   - In the **Provider type** list, select **Oracle JDBC Driver**.
   - In the **Implementation type** list, select **Connection pool data source**.
7. Click **Next** and, in the Step 2 pane, accept the default database class path and click **Next** again.
8. In the Step 3 pane, click **Finish**.
9. Click **Save directly to master configuration**.

➤ **To create the Oracle JDBCdata source:**

1. In the navigation tree, click **Resources** > **JDBC** > **JDBC Providers** and, in the right pane, click the provider you created in "To install the Oracle 10g database driver:" on page 28.
2. Under Additional Properties, click **Data sources** and then click **New**.
3. In the Step 1 pane, set the following configurations and then click **Next**:
   - In the **Data source name**, type `IDP_DS`.
   - In the **JNDI name**, type `IDP_DS`.
   - In the list, under Component-Managed Authentication and XA Recovery Authentication, select the authentication alias created for this data source in "To create a J2C authentication configuration for the data source:" on page 22.

4. In the Step 2 pane, type the following line in the **URL** field, and then click **Next**:

   `jdbc:oracle:thin:@[server_host]:[port]:[SID]`

   where *[server_host]* is the IP address of the database server, *[port]* is the port on which the database is listening (default 1521), and *[SID]* is the service ID of the database.

5. In the Step 3 pane, click **Finish**.

6. Click **Save directly to master configuration**.

7. Select the data source you just created to modify additional parameters and set the following configuration:

   - In the **Container-managed authentication alias** list, select the authentication alias created for this data source in "To create a J2C authentication configuration for the data source:" on page 22.
   - In the **Mapping-configuration alias** list, select DefaultPrincipalMapping.

8. Click **OK** or **Apply**.

9. Click **Save directly to master configuration**.

➤ **To configure IDP_DS connection pools:**

1. In the navigation tree, click **Resources** > **JDBC** > **JDBC Providers** and, in the right pane, click the **Oracle JDBC Driver** data source you just created.

2. Under Additional Properties, click **Data sources** and then select **IDP_DS**.

3. On the next screen, under Additional Properties, click **Connection Pool Properties** and, in the **Maximum connections** box, type `100`.

4. Click **OK** or **Apply**.

5. Click **Save directly to master configuration**.

➤ **To create the Oracle JDBCdata source for LiveCycle Rights Management ES:**

Note: This section applies only if you have installed Rights Management ES.

1. In the navigation tree, click **Resources** > **JDBC** > **JDBC Providers** and, in the right pane, click the provider you created in "To install the Oracle 10g database driver:" on page 28.

2. Under Additional Properties, click **Data sources** and then click **New**.

3. In the Step 1 pane, set the following configurations and then click **Next**:

   - In the **Data source name** box, type `RM_DS`.
   - In the **JNDI name** box, type `EDC_DS`.
   - In the list, under Component-Managed Authentication and XA Recovery Authentication, select the authentication alias created for this data source in "To create a J2C authentication configuration for the data source:" on page 22.

4. In the Step 2 pane, type the following line in the **URL** field, and then click **Next**:

   `jdbc:oracle:thin:@[server_host]:[port]:[SID]`

   where *[server_host]* is the IP address of the database server, *[port]* is the port on which the database is listening (default 1521), and *[SID]* is the service ID of the database.

5. In the Step 3 pane, click **Finish**.

6. Click **Save directly to master configuration**.

7. Select the data source you just created to modify additional parameters.

8. Set the following configuration and then click **OK**:

   - In the **Container-managed authentication alias** list, select the authentication alias created for this data source in "To create a J2C authentication configuration for the data source:" on page 22.
   - In the **Mapping-configuration alias** list, select DefaultPrincipalMapping.

9. Click **Save directly to master configuration**.

➤ **To configure IDP_DS connection pools for LiveCycle Rights Management ES:**

Note: This section applies only if you have installed Rights Management ES.

1. In the navigation tree, click **Resources** > **JDBC** > **JDBC Providers** and, in the right pane, click the **Oracle JDBC Driver** data source you just created.

2. Under Additional Properties, click **Data sources** and then select **RM_DS**.

3. On the next screen, under Additional Properties, click **Connection Pool Properties** and, in the **Maximum connections** box, type `30`.

4. Click **OK** or **Apply**.

5. Click **Save directly to master configuration**.

Configuring the SQL Server data source

Configuring the SQL Server data source requires you to install the SQL Server database drivers, create a SQL Server JDBC provider on WebSphere, create the data source on WebSphere, and then configure the corresponding connection pool.

➤ **To install the SQL Server database driver:**

- If you have not done so already, download and install the SQL Server 2005 JDBC Driver 1.1 from the following Microsoft site by following the website instructions:

  http://www.microsoft.com/downloads/details.aspx?familyid=6d483869-816a-44cb-9787-a866235efc7c&displaylang=en

  Note: Make note of the directory location where you install the driver on your system.

➤ **To create the SQL Server 2005 JDBC provider:**

1. In the WebSphere Administrative Console navigation tree, click **Environment** > **Websphere Variables** and, in the right pane, click **MSSQLSERVER_JDBC_DRIVER_PATH**.
2. Under General Properties, in the **Value** box, type the path to the sqljdbc.jar file you created in "To install the SQL Server database driver:" on page 30 and then click **OK**.
3. In the **Messages** box, click **Save directly to master configuration**.
4. In the navigation tree, click **Resources** > **JDBC** > **JDBC Providers**.
5. In the drop-down list in the right pane, select **Node** (without server) as the level, and then click **New**.
6. In Step 1 pane, set the following configurations and then click **Next**:
   - In the **Database type** list, select `User-defined`.
   - In the **Implementation class name** box, type `com.microsoft.sqlserver.jdbc.SQLServerConnectionPoolDataSource`.
   - In the **Name** box, type `User-defined JDBC Provider` (default).
7. In the Step 2 pane, set the class path configuration as follows and then click **Next**:

   `${MSSQLSERVER_JDBC_DRIVER_PATH)/sqljdbc.jar`
8. In the Step 3 pane, click **Finish**.
9. Click **Save directly to master configuration**.

➤ **To create the SQL Server 2005 data source:**

1. In the navigation tree, click **Resources** > **JDBC** > **JDBC Providers** and, in the right pane, click the provider you created in "To create the SQL Server 2005 JDBC provider:" on page 31.
2. Under Additional Properties, click **Data sources** and then click **New**.
3. In the Step 1 pane, set the following configurations and then click **Next**:
   - In both the **Data source name** box and the **JNDI name** box, type `IDP_DS`.
   - In the list under Component-Managed Authentication and XA Recovery Authentication Alias, select the authentication alias created for this data source in "To create a J2C authentication configuration for the data source:" on page 22.
4. In the Step 2 pane, accept the default data store helper class and click **Next**.
5. In the Step 3 pane, click **Finish**.
6. Click **Save directly to master configuration**.
7. Select the data source you just created to modify additional parameters.
8. Set the following configuration and then click **OK**:
   - In the **Container-managed authentication alias** list, select the authentication alias created for this data source in "To create a J2C authentication configuration for the data source:" on page 22.
   - In the **Mapping-configuration alias** list, select DefaultPrincipalMapping.
9. Click **Save directly to master configuration**.

➤ **To configure IDP_DS connection pools:**

1. In the navigation tree, click **Resources** > **JDBC** > **JDBC Providers** and, in the right pane, click the **User-defined JDBC Driver** data source you just created.
2. Under Additional Properties, click **Data sources** and then select **IDP_DS**.
3. On the next screen, under Additional Properties, click **Custom Properties,** and then click **New**.
4. Under DB2 Universal Data Source Properties, type the database name and server name:
   - In the **Database name** box, type *database_name*.
   - In the **Server name** box, type the IP address of SQL Server database.
5. Click **OK** or **Apply**.
6. Click **Save directly to master configuration**.
7. In the navigation tree, click **Resources** > **JDBC** > **JDBC Providers** and, in the right pane, click the **User-defined JDBC Driver** data source you just created.
8. Under Additional Properties, click **Data sources** and then select **IDP_DS**.
9. On the next screen, under Additional Properties, click **Connection Pool Properties** and, in the **Maximum connections** box, type `100`.
10. Click **OK** or **Apply**.
11. Click **Save directly to master configuration**.

➤ **To create the SQL Server 2005 data source for LiveCycle Rights Management ES:**

Note: This section applies only if you have installed Rights Management ES.

1. In the navigation tree, click **Resources** > **JDBC** > **JDBC Providers** and, in the right pane, click the provider you created in "To create the SQL Server 2005 JDBC provider:" on page 31.
2. Under Additional Properties, click **Data sources** and then click **New**.
3. In the Step 1 pane, set the following configuration and then click **Next**:
   - In the **Data source name** box, type `RM_DS`.
   - In the **JNDI name** box, type `EDC_DS`.
   - In the list under Component-Managed Authentication and XA Recovery Authentication Alias, select the authentication alias created for this data source in "To create a J2C authentication configuration for the data source:" on page 22.
4. In the Step 2 pane, accept the default data store helper class and click **Next**.
5. In the Step 3 pane, click **Finish**.
6. Click **Save directly to master configuration**.

➤ **To configure IDP_DS connection pools for LiveCycle Rights Management ES:**

Note: This section applies only if you have installed Rights Management ES.

1. In the navigation tree, click **Resources** >**JDBC** > **JDBC Providers** and, in the right pane, click the **User-defined JDBC Driver** data source you just created.
2. Under Additional Properties, click **Data sources** and then select **RM_DS**.
3. On the next screen, under Additional Properties, click **Custom Properties** and then click **New**.
4. Provide the appropriate information in these boxes:

   Alias: Type a name appropriate for the database user (for example, type `IDP_DS/db2-db2user`).

   User ID: Enter a user ID. This ID is the login credential used to access whichever database will be used with the IDP_DS data source (for example, db2user).

   Password: Type a password for this user.
5. Click **OK** or **Apply**.
6. Click **Save directly to master configuration**.
7. In the navigation tree, click **Resources** > **JDBC** > **JDBC Providers** and, in the right pane, click the **User-defined JDBC Driver** data source you just created.
8. Under Additional Properties, click **Data sources** and then select **RM_DS**.
9. On the next screen, under Additional Properties, click **Connection Pool Properties** and, in the **Maximum connections** box, enter `30`.
10. Click **OK** or **Apply**.
11. Click **Save directly to master configuration**.

➤ **To use integrated security to make a trusted connection with SQL Server:**

1. In the navigation tree, click **Resources** > **JDBC** > **Data Sources** and, in the right pane, click **IDP_DS**.
2. In the right pane, under Additional Properties, click **Custom Properties**, and then click **New**.
3. In the **Name** box, type `integratedSecurity` and, in the **Value** box, type `true`.
4. In the navigation tree, click **Resources** > **JDBC** > **Data Sources** and, in the right pane, click **RM_DS**.
5. In the right pane, under Additional Properties, click **Custom Properties**, and then click **New**.
6. In the **Name** box, type `integratedSecurity` and, in the **Value** box, type `true`.

   You can leave the
7. On the computer where WebSphere is installed, add the sqljdbc_auth.dll file to the Windows systems path (C:\Windows). The sqljdbc_auth.dll file is in the same location as the Microsoft SQL JDBC 1.1 driver installation (default is *[InstallDir]*/sqljdbc_1.1/enu/auth/x86).
8. In the Windows Control Panel under Services, right-click the Windows service for WebSphere (IBM WebSphere Application Server V6.1 - <node>) and select **Properties**.

9. In the properties dialog box, click the **Log On** tab.
10. Select the **This Account** option, and provide the information required to set the log in account you want to use.
11. Set Security on SQL Server from **Mixed** mode to **Windows Authentication only**.

Configuring JMS resources for WebSphere

You must configure Java Message Service (JMS) resources for WebSphere.

➤ **To create the IDP_JMS_Bus:**

1. In the WebSphere Administrative Console navigation tree, click **Service Integration** > **Buses** and, in the right pane, click **New**.
2. In the Step 1 pane, type `IDP_JMS_Bus` in the box provided.
3. Click **Next** and then click **Finish** on the screen that follows.
4. In the **Messages** box, click **Save directly to master configuration**.

➤ **To assign bus members:**

1. In the navigation tree, click **Service Integration** > **Buses** and, in the right pane, click **IDP_JMS_Bus**.
2. Under Topology, click **Bus Members** and then click **Add**.
3. In the Step 1 pane, ensure that **Server** is selected and then click **Next**.
4. In the Step 2 pane, select **Data store** and click **Next**.
5. In the Step 3 pane, select **Create default data source with generated JNDI name** and click **Next**.
6. Click **Finish**, and then click **Save directly to master configuration**.

Note: After you restart the application server, you can test whether the messaging bus has been started correctly by navigating to **Service Integration** > **Buses**, clicking **IDP_JMS_Bus**, and then clicking **Messaging engines** under Topology. A green symbol is displayed to show that a messaging bus is functioning.

➤ **To configure JMS queue connection factories:**

1. In the navigation tree, click **Resources** > **JMS** > **Queue connection factories**.
2. In the drop-down list in the right pane, select **Node** (without server) as the level, and then click **New**.
3. Select **Default messaging provider** and click **OK**.
4. In the Administration area, set these properties:
   - In the **Name** box, type `QueueConnectionFactory`.
   - In the **JNDI name** box, type `QueueConnectionFactory`.
5. In the Connection area, in the **Bus name list**, select **IDP_JMS_Bus**.

6. In the Quality of Service area, set these properties:
   - In the **Non persistent message reliability** list, select **As bus destination**.
   - In the **Persistent message reliability** list, select **As bus destination**.
7. In the Advanced Administrative area, select the appropriate XA recovery authentication alias as defined in "To create a J2C authentication configuration for the data source:" on page 22.
8. Click **OK** or **Apply**.
9. Click **Save directly to master configuration**.
10. In the list, click **QueueConnectionFactory** and, under Additional Properties, click **Connection pool properties**.
11. On the next screen, under General Properties, set the following properties:
    - In the **Maximum connections** box, type `50`.
    - In the **Minimum connections** box, type `10`.
12. Click **OK** or **Apply**.
13. Click **Save directly to master configuration**.
14. Repeat steps 2 through 13 to create another JMS queue connection factory, replacing **QueueConnectionFactory** with **JobManagerQueueConnectionFactory** in step 5 for both the name and JNDI name.

➤ **To configure JMS topic connection factories:**

1. In the navigation tree, click **Resources** > **JMS** > **Topic connection factories**.
2. In the drop-down list in the right pane, select **Node** (without server) as the level, and then click **New**.
3. Select **Default messaging provider** and click **OK**.
4. In the Administration area, set these properties:
   - In the **Name** box, type `TopicConnectionFactory`.
   - In the **JNDI name** box, type `TopicConnectionFactory`.
5. In the Connection area, in the **Bus name list**, select **IDP_JMS_Bus**.
6. In the Quality of Service area, set these properties:
   - In the **Non persistent message reliability** list, select **As bus destination**.
   - In the **Persistent message reliability** list, select **As bus destination**.
7. In the Advanced Administrative area, select the appropriate XA recovery authentication alias as defined in "To create a J2C authentication configuration for the data source:" on page 22.
8. Click **OK** or **Apply**.
9. Click **Save directly to master configuration**.
10. In the list, click **TopicConnectionFactory** and, under Additional Properties, click **Connection Pool Properties**.

11. On the next screen, under General Properties, set the following properties:
    - In the **Maximum connections** box, type `50`.
    - In the **Minimum connections** box, type `10`.
12. Click **OK** or **Apply**.
13. Click **Save directly to master configuration**.
14. Repeat steps 3 through 13 to create another connection factory, replacing TopicConnectionFactory with JobManagerTopicConnectionFactory in step 4 for both the name and JNDI name.

➤ **To create a queue:**

1. In the navigation tree, click **Resources** > **JMS** > **Queues**.
2. In the drop-down list in the right pane, select **Node** (without server) as the level, and then click **New**.
3. Accept the default or select **Default messaging provider** and then click **OK**.
4. In the Administration area, set these properties:
    - In the **Name** box, type `queue/adobe_PECommandQueue`.
    - In the **JNDI name** box, type `queue/adobe_PECommandQueue`.
5. In the Connection area, set the properties as follows:
    - In the **Bus name** list, select **IDP_JMS_Bus**.
    - In the **Queue name** list, select **other, please specify** and then type `adobe_PECommandQueue` in the box that appears.
    - In the **Delivery mode** list, select **Persistent**.
6. In the Advanced area, in the **Read ahead** list, select **Inherited from connection factory**.
7. Click **OK** or **Apply**.
8. Click **Save directly to master configuration**.
9. Repeat steps 3 through 8 for each of the queues in the following table, replacing the properties under the Connection group set in step 5 with the appropriate values.

Name	Delivery Mode	JNDI name
adobe_PEDCommandQueue	persistent	queue/adobe_PEDCommandQueue
adobe_PEInteractionQueue	persistent	queue/adobe_PEInteractionQueue
adobe_JobManagerQueue	persistent	queue/adobe_JobManagerQueue

Next, you must create a bus destination for each queue defined in "To create a queue:" on page 36.

➤ **To create a bus destination:**

1. In the navigation tree, click **Service Integration** > **Buses** and, in the right pane, click **IDP_JMS_Bus**.
2. On the next screen, under Destination Resources, click **Destinations**, and then click **New**.

3. On the next screen, under Select Destination Type, select **Queue** and then click **Next**.
4. In the step 1 pane, in the **Identifier** box, type `adobe_PECommandQueue` and then click **Next**.
5. Click **Next**, and then click **Finish**.
6. Click **Save directly to master configuration**.
7. Repeat steps 3 through 6 for each queue defined in "To create a queue:" on page 36.

➤ **To create the first topic:**

1. In the navigation tree, click **Resources** > **JMS** > **Topics**.
2. In the drop-down list in the right pane, select **Node** (without server) as the level, and then click **New**.
3. Accept the default or select **Default messaging provider** and click **OK**.
4. In the Administration area, set these properties:
   - In the **Name** box, type `adobe_LAFEventTopic`.
   - In the **JNDI name** box, type `topic/adobe_LAFEventTopic`.
5. In the Connection area, set the properties as follows:
   - In the **Topic name** box, type `adobe_LAFEventTopic`.
   - In the **Bus name** list, select **IDP_JMS_Bus**.
   - In the **Topic space** list, select **Default.Topic.Space**.
6. Click **OK** or **Apply**.
7. Click **Save directly to master configuration**.
8. Repeat steps 1 through 7 for the queue in the following table, replacing the Name, JDNI name and Topic name properties.

Name and topic name	Delivery Mode	JNDI name
adobe_TaskEventTopic	persistent	topic/adobe_TaskEventTopic

Assigning JMS Activation Specification

➤ **To create PECommand_AS:**

1. In the WebSphere Administrative Console navigation tree, click **Resources** > **JMS** > **Activation specifications**.
2. In the drop-down list in the right pane, select **Node** (without server) as the level, and then click **New**.
3. Accept the default or select **Default messaging provider** and click **OK**.
4. In the Administration area, set these properties:
   - In the **Name** box, type `PECommand_AS`.
   - In the **JNDI name** box, type `PECommand_AS`.

5. In the Destination area, set the properties as follows:
   - In the **Destination type** list, select **Queue**.
   - In the **Destination JNDI name** box, type `queue/adobe_PECommandQueue`.
   - In the **Bus name** list, select **IDP_JMS_Bus**.
6. Click **OK** or **Apply**.
7. In the **Messages** box, click **Save directly to master configuration**.

➤ **To create Task_Event_AS:**

1. In the navigation tree, click **Resources** > **JMS** > **Activation specifications**.
2. In the drop-down list in the right pane, select **Node** (without server) as the level, and then click **New**.
3. Accept the default or select **Default messaging provider** and click **OK**.
4. In the Administration area, set these properties:
   - In the **Name** box, type `Task_Event_AS`
   - In the **JNDI name** box, type `Task_Event_AS`
5. In the Destination area, set the properties as follows:
   - In the **Destination type** list, select **Topic**.
   - In the **Destination JNDI name** box, type `topic/adobe_TaskEventTopic`
   - In the **Bus name** list, select **IDP_JMS_Bus**.
6. Click **OK** or **Apply**.
7. Click **Save directly to master configuration**.

➤ **To create JobManager_AS:**

1. In the navigation tree, click **Resources** > **JMS** > **Activation specifications**.
2. In the drop-down list in the right pane, select **Node** (without server) as the level, and then click **New**.
3. Accept the default or select **Default messaging provider** and click **OK**.
4. In the Administration area, set these properties:
   - In the **Name** box, type `JobManager_AS`.
   - In the **JNDI name** box, type `JobManager_AS`.
5. In the Destination area, set the properties as follows:
   - In the **Destination type** list, select **Queue**.
   - In the **Destination JNDI name** box, type `queue/adobe_JobManagerQueue`
   - In the **Bus name** list, select **IDP_JMS_Bus**.
6. Click **OK** or **Apply**.
7. Click **Save directly to master configuration**.

Configuring J2C authentication for JMS

This section outlines how to set J2C authentication.

Note: This procedure is required only for WebSphere installations where administrative security is enabled. When your application server is configured to enable administrative security, you must create the JMS group, JMS user, associating security, and assigning group privileges.

➤ **To configure J2C authentication:**

1. In the WebSphere Administrative Console navigation tree, click **Security** > **Secure administration**, **applications** > **infrastructure**.
2. Under Authentication, click **Java Authentication and Authorization Service** > **J2C authentication data**, and then click **New**.
3. Provide the appropriate information in these boxes:

   Alias: Type a name appropriate for the database user (for example, type `IDP_DS/db2-db2user`).

   User ID: Enter a user ID. This ID is the login credential used to access whichever database will be used with the IDP_DS data source (for example, db2user).

   Password: Type a password for this user.
4. Click **OK** or **Apply**.
5. In the **Messages** box, click **Save directly to master configuration**.

➤ **To create a group:**

1. In the navigation tree, click **User and Groups** > **Manage Groups**, and then click **Create**.
2. In the **Group name** box, type `lc8_jms_group`, and then click **Create**.

➤ **To create a user:**

1. In the navigation tree, click **User and Groups** > **Manage Users**, and then click **Create**.
2. Click **Group Membership** and click **Search**.
3. Select the group name **lc8_jms_group** that was previously created and click **Close**.
4. In the **User ID** box, type *`[authentication for JAAS name]`*.
5. Add a first and last name in the boxes provided.
6. Type the *[JAAS authentication name]* as the password, and then click **create**.

➤ **To associate security:**

1. In the navigation tree, click **Resources** > **JMS** > **Activation specifications**.
2. Click one of the activation specifications.
3. Under Additional, in the **Authentication Alias** list, select the JMS authentication alias that was created in "To configure J2C authentication:" on page 39.

4. Click **OK** or **Apply**.
5. Click **Save directly to master configuration**.
6. Repeat steps 1 to 5 for all activation specifications.

➤ **To assign group privileges to the IDP_JMS Bus:**

1. In the navigation tree, click **Service Integration** > **Buses** and, in the right pane, click **IDP_JMS Bus**.
2. Under Additional Properties, click **Security**.
3. Under Additional Properties, click **Users and groups in the bus connector role**.
4. In **Bus Connector Role group**, use the default or select **Group name** and type the group name created in "To configure J2C authentication:" on page 39.
5. Click **OK** or **Apply**.
6. Click **Save directly to master configuration**.

SQL Server JMS validation

Note: Validation is required only for Microsoft SQL Server.

The SQL Server JMS setup requires additional verification. This is also required if the JMS/LCM verification fails.

➤ **To verify the JMS setup with SQL Server:**

1. In the WebSphere Administrative Console navigation tree, click **Service Integration** > **Buses** and, in the right pane, click **IDP_JMS_BUS**.
2. Under Topology, click **Messaging Engines**. When working, it should display a green arrow. The status for the bus is likely unknown at this point.
3. Select your messaging engine.
4. Under Additional Properties, click **Message store.** The schema name must match the user name; if it does not, set it to match. To set up the Microsoft SQL Server database and users, see *Preparing to Install LiveCycle ES* at www.adobe.com/go/learn_lc_prepareInstall.
5. In the **Messages** box, click **Save directly to master configuration**.
6. Delete any tables that begin with **SIB** to ensure there are no conflicts with old bus configurations.
7. Restart WebSphere and retry step 1 to ensure that the bus is running.

Restart WebSphere

Restart your WebSphere Application Server for all configuration changes to take affect.

Next step

If you performed these configuration steps partway through the LiveCycle Configuration Manager configuration and upgrade process, you can now return to LiveCycle Configuration Manager and continue on to migrate essential data. (See step 32 on page 48.)

If you performed these steps in preparation for upgrading, you can now run LiveCycle Configuration Manager to configure, upgrade, and deploy LiveCycle ES. (See "Configuring LiveCycle ES for Deployment" on page 42.)

4 Configuring LiveCycle ES for Deployment

This chapter describes how to use LiveCycle Configuration Manager to perform any of the following tasks:

- Configure LiveCycle ES solution components in an EAR file for deploying to the application server
- Configure application server properties to support LiveCycle ES
- Validate application server configuration
- Deploy LiveCycle ES EAR files
- Initialize theLiveCycle ES database
- Deploy LiveCycle ES component
- Validate the LiveCycle ES component deployment
- Configure the Reader Extensions ES Rights credential (if Reader Extensions ES is installed)
- Initialize BAM metadata for Business Activity Monitoring ES (if Business Activity Monitoring ES is installed)
- (Optional) Import the LiveCycle ES Samples.

The following upgrade tasks are also performed when you select the Upgrade from LiveCycle 7.x task:

- Apply LiveCycle 7.x configuration to LiveCycle ES
- Migrate data essential to LiveCycle ES operation
- Migrate remaining data (for LiveCycle Policy Server upgrades only)

This chapter assumes that you have prepared your environment for hosting LiveCycle ES and installed the solution component files. If you have not done this, see *Preparing to Upgrade to LiveCycle ES* at http://www.adobe.com/go/learn_lc_upgradePreparation and "Installing the Solution Component Files" on page 15.

Note: If the application server targeted for LiveCycle ES is installed on the same computer as the LiveCycle 7.x application server, and you want to configure the application server manually rather than have LiveCycle Configuration Manager do the task, you will be prompted part way through the configuration and upgrade process to stop the LiveCycle 7.x server. You must then start WebSphere and configure it as described in "Manually Configuring WebSphere" on page 21. Then you can proceed with the upgrade and deployment in LiveCycle Configuration Manager.

If the LiveCycle 7.x and LiveCycle ES application servers are installed on separate computers, you should complete all the application server configuration tasks before you start LiveCycle Configuration Manager so that the LiveCycle ES and migrated data can be deployed immediately.

About LiveCycle Configuration Manager

LiveCycle Configuration Manager is a wizard-like tool used to configure, deploy, and validate LiveCycle ES components for deployment to the application server. You can optionally use LiveCycle Configuration Manager to configure the application server and deploy the product EAR files to the application server.

LiveCycle Configuration Manager is installed with the solution component files when you run the LiveCycle ES installation program. When you run LiveCycle Configuration Manager, you specify the LiveCycle ES solution components you are configuring, as well as the tasks you want LiveCycle Configuration Manager to perform.

You can start LiveCycle Configuration Manager from the installation program to configure solution components during the installation process, or you can start LiveCycle Configuration Manager any time after the installation. If you are planning to use LiveCycle Configuration Manager to configure the application server or deploy to the application server, the application server must be started so that LiveCycle Configuration Manager can perform configuration tasks on it.

You can configure an application server that is installed on a different computer than the one on which you are running LiveCycle Configuration Manager. However, an application server must also be installed (but does not have to be running) on the computer running LiveCycle Configuration Manager so that LiveCycle Configuration Manager can use the application server library files.

Determining the application server SOAP port

Some LiveCycle Configuration Manager screens require you to provide the SOAP port of the application server. Use the procedures in this topic to determine which port is used for SOAP connections with the application server. The default port is 8880.

➤ **To determine the SOAP port on WebSphere:**

1. In the navigation panel of the WebSphere Administrative Console, click **Servers** > **Application Servers** > ***[serverName]*** > **Communications** > **Ports**.

2. Take note of the value in the **SOAP_CONNECTOR_ADDRESS** box.

Configuring, upgrading to, and deploying LiveCycle ES

Now that LiveCycle ES is installed, you are ready to run LiveCycle Configuration Manager to upgrade from LiveCycle 7.x to LiveCycle ES. LiveCycle Configuration Manager performs the tasks required for upgrading, including extracting the required data and properties from the LiveCycle 7.x configuration and applying it to the LiveCycle ES configuration.

These instructions assume you have already installed the application server and either set up a supported database or migrated the LiveCycle 7.x database to a new database required for LiveCycle ES according to the instructions in *Preparing to Upgrade to LiveCycle ES* at http://www.adobe.com/go/learn_lc_upgradePreparation. If the application server for LiveCycle ES is installed on the same computer as LiveCycle 7.x server, you will be prompted when you can stop the LiveCycle 7.x server and configure the LiveCycle ES application server and start it.

When you run LiveCycle Configuration Manager, you can select the tasks that you want the program to perform automatically.

Note: Using LiveCycle Configuration Manager to deploy LiveCycle ES solution components to remote servers is supported only for managed application servers, not for stand-alone application servers.

Tip: LiveCycle Configuration Manager verifies the values specified on each screen when you click Next. If it cannot validate a value, a warning a warning message appears, the property on the screen turns red, and you cannot proceed until you enter a valid value.

When Configuration Manager completes the configuration of LiveCycle ES, it places the files to be deployed (adobe-livecycle-nativewebsphere-*[OS]*.ear, adobe-livecycle-websphere.ear, and adobe-workspace-client.ear if you LiveCycle installed Process Management ES) to the application server in the following directory:

- (Windows) *[LiveCycleES root]*\configurationManager\export
- (Linux, UNIX) *[LiveCycleES root]*/configurationManager/export

If you plan to manually deploy LiveCycle ES to the application server, you can access the files in the /configurationManager/export directory.

Note: If you have previously deployed LiveCycle ES files, you must first undeploy the product EAR files from the application server. However, if you use LiveCycle Configuration Manager to deploy EAR files, it automatically undeploys previously deployed files before deploying updated ones.

If you are configuring a remote application server, ensure that an application server is also installed on the same computer as LiveCycle Configuration Manager so that LiveCycle Configuration Manager can use the application server library files.

➤ **To configure, upgrade to, and deploy LiveCycle ES:**

Tip: You can press **F1** in LiveCycle Configuration Manager to view Help information for the screen you are viewing. This Help contains details that may not be included in this document, and are specific to the context of each screen in LiveCycle Configuration Manager.

1. If you did not start LiveCycle Configuration Manager automatically from the installation program, navigate to the *[LiveCycleES root]*/configurationManager/bin directory and entering the following command:
   - (Windows) `ConfigurationManager.bat`
   - (Linux, UNIX) `./ConfigurationManager.sh`
2. On the Welcome screen, click **Next**.
3. Select **Upgrade from LiveCycle 7.x**. All the subtasks are selected by default. You can leave all the tasks selected or deselect a task if you do not want to perform it now. Some conditions apply for deselecting tasks described in this list:

   Apply LiveCycle 7.x configuration to LiveCycle ES: Retrieves all required data from LiveCycle 7.x files (deployable modules) and applies this data to the deployable LiveCycle ES components. You must complete this task before you can migrate data to LiveCycle ES. The following two tasks are depend on this task being selected or already completed.

   Migrate data essential to LiveCycle ES operation: Imports essential data files, such as custom fonts and files into the global document storage directories and LiveCycle Policy Server policies, configuration settings, watermarks, document licenses, revocation information and external users into LiveCycle ES. To complete this task, you are prompted to stop the LiveCycle 7.x server. When LiveCycle Configuration Manager completes migrating the data, LiveCycle ES can begin accepting requests.

   Migrate remaining data: Imports additional non-essential data, such as audit records associated with LiveCycle Policy Server, from LiveCycle 7.x to LiveCycle ES. The task is only relevant to upgrading LiveCycle Policy Server. The LiveCycle ES server can continue to take requests during this task. This task may require a significant amount of time to complete. You can deselect this task for the initial installation and upgrade, and return to LiveCycle Configuration Manager at a later time to complete the migration.

4. Click **Next** to continue.

5. On the Solution Component Selection screen, select the LiveCycle ES solution components that you have installed and plan to deploy.

6. On the Product Upgrade Selection screen, ensure that the products you want to upgrade are selected. The products that are preselected on the Product Upgrade Selection screen indicate the LiveCycle 7.x equivalents that can be upgraded. If a product that you are planning to upgrade is not available for selection, ensure that the corresponding solution components is selected on the previous screen.

   Note: If you are upgrading LiveCycle Forms 7.x, LiveCycle Print 7.x, or LiveCycle PDF Generator 7.x to LiveCycle Forms ES, LiveCycle Output ES, or LiveCycle PDF Generator ES respectively, then LiveCycle Assembler 7.x is selected by default. If you are not upgrading LiveCycle Assembler 7.x, you must deselect it.

7. On the Task Selection screen, select all the tasks you want to perform, and click **Next**.

   Note: If you do not want to configure the application server and deploy LiveCycle ES using LiveCycle Configuration Manager, do not select the **Configure Application Server** and **Validate Application Server Configuration** tasks.

8. ***(Not applicable for LiveCycle Policy Server upgrade)*** On the Import LiveCycle 7.x Files screen, provide the path to the deployable archive files associated with LiveCycle 7.x. You exported these files in the preparation phase to ensure that you are using the most current version of the files. (See *Preparing to Upgrade to LiveCycle ES* at http://www.adobe.com/go/learn_lc_upgradePreparation.) If you have both the Adobeservices.sar and LiveCycle.ear files in your liveCycle 7.x deployment, import the LiveCycle.ear file. When you have provided the required information, click **Next**.

   Note: The fields are enabled based on the products you selected for upgrading on the previous screen. All enabled fields are required, and the specific file name depends on the version of LiveCycle 7.x you are upgrading from.

Tip: Press **F1** to view a list of the expected file names, according to the version of LiveCycle you are upgrading from. You can also move your pointer over the fields to display tool tips that contain lists of the possible file names. These expected file names are only defaults. Any file that matches the applicable file type filter (.war, .bar, .sar, .ear) is accepted.

9. ***(Not applicable for LiveCycle Policy Server upgrade)*** On the Extract LiveCycle 7.x Configuration Data screen, click **Start**. When the extraction has completed successfully, click **Next**.

10. On the Configure LiveCycle ES screen, click **Configure**. When the EAR files have been configured, click **Next**.

11. ***(Not applicable for LiveCycle Policy Server upgrade)*** On the Apply LiveCycle 7.x Configuration Data screen, click **Start**. When the task has completed successfully, click **Next**.

12. ***(Not applicable for LiveCycle Policy Server upgrade)*** On the Copy Shared Compatibility Layer screen, you must perform a manual step outside of LiveCycle Configuration Manager. Copy the adobe-bmc-client.jar file from *[LiveCycleES root]*/LiveCycle_ES_SDK/client-libs/common directory to the *[appserver domain]*/lib directory.

    When you have finished copying the adobe-bmc-client.jar, click **Next**.

13. On the Copy LiveCycle 7.x Customer Fonts screen, select the option to automatically place the fonts into the LiveCycle ES customer fonts directory. By selecting this option, you do not have to manually copy the fonts later in the process. This screen only displays if LiveCycle Configuration Manager detects custom fonts on the server. If you are not using additional fonts, go to step 15.

14. Specify a location for the customer fonts directory in the second text field (for example, *[LiveCycleES root]*/customerFonts), and then click **Next**.

    Note: The customer fonts directory is used to store fonts that are not provided as part of the LiveCycle installation.

    Your right to use fonts provided by parties other than Adobe is governed by the license agreements provided to you by such parties in connection with those fonts, and is not covered under your license to use Adobe software. Adobe recommends that you review and ensure you are in compliance with all applicable non-Adobe license agreements before using non-Adobe fonts with Adobe software, particularly with respect to use of fonts in a server environment.

15. On the Configure LiveCycle ES (continued) screen, set the directories that LiveCycle ES will use to access fonts and store temporary data associated with processing jobs:
    - (Optional) To change the default locations of the Adobe Server Fonts directory, type the path or browse to the directory.
    - Accept the value in the **Customer Fonts directory** box.
    - (Optional) To change the default locations of the System Fonts directory, type the path or browse to the directory.
    - (Optional) To specify the location of the Temp directory, click **Browse**.
    - To specify the locations of the Global document storage root directory, click **Browse**. (You determined the location of the Global document storage directory during the directory back-up process. See "Backing Up LiveCycle 7.x Environment" in the *Preparing to Upgrade to LiveCycle ES* at http://www.adobe.com/go/learn_lc_upgradePreparation document.)
    - To enable FIPS, ensure that **Enable FIPS** is selected. Select this option only if you require the Federal Information Processing Standards (FIPS) to be enforced.

16. Click **Configure** to configure the directories. When the configuration is complete, click **Next**.

    Note: The next screen only appears when the Global document storage directory specified for LiveCycle ES is different than that specified for LiveCycle 7.x, and the servers are located on different hosts.

17. The Configuring Document Manager screen prompts you to copy the contents of the Global document storage directory used for LiveCycle 7.x to the Global document storage directory that will be used by LiveCycle ES server. Without exiting LiveCycle Configuration Manager, navigate to the LiveCycle 7.x Global document storage directory shown on the LiveCycle Configuration Manager screen. Copy all the contents of this directory to the LiveCycle ES Global document storage directory, which is also shown on the LiveCycle Configuration Manager screen. Click **Next**.

18. On the Configure LiveCycle ES Summary screen, click **Next**.

19. On the Configure LiveCycle ES Connectors screen, press **F1** and follow the instructions in the Help dialog box.

20. ***(LiveCycle PDF Generator ES only)*** On the LiveCycle 7.x Database screen, provide the following information about your LiveCycle 7.x database so that LiveCycle Configuration Manager can connect to it.

    Database Type: The type of database you are using as the LiveCycle 7.x database.

    Database Name: The name of the LiveCycle 7.x database you are connecting to. Reselect the database to ensure that the JDBC driver field (below) shows the default driver.

    Host: The name or IP address of the computer that hosts the LiveCycle 7.x database server.

Port: The port used to access the database service. The port number listed is the default for the database type you selected. If you are using a non-default port number for the database, enter it here.

User: The name of the user account that accessed the database server specified in the database name entered above (the database you created for LiveCycle 7.x).

Password: The password for the user account specified for the database name you entered above.

JDBC driver: The location of the JDBC driver installed with LiveCycle ES and used to connect to the LiveCycle 7.x database. The drivers (except for those for SQL Server) are included in the LiveCycle ES installation and are located in the *[LiveCycleES root]*/lib/db directory. You must obtain the that the SQL Server driver from the Microsoft web site, and therefore this driver is located in the place where you saved it. See "Creating a SQL Server database" in *Preparing to Upgrade to LiveCycle ES* at http://www.adobe.com/go/learn_lc_upgradePreparation.

21. ***(LiveCycle Policy Server upgrade only)*** On the LiveCycle Policy Server 7.x Database screen, provide information about your LiveCycle Policy Server 7.x database so that LiveCycle Configuration Manager can connect to it:

    Database Type: The type of database you are using as the LiveCycle Policy Server 7.x database.

    Database Name: The name of the LiveCycle Policy Server 7.x database you are connecting to. Reselect the database to ensure that the JDBC driver field (below) shows the default driver.

    Host: The name or IP address of the computer that hosts the LiveCycle Policy Server 7.x database server. (Use the name only if it can be resolved.)

    Port: The port used to access the database service. The port number listed is the default for the database type you selected. If you are using a non-default port number for the database, enter it here.

    User: The name of the user account that accessed the database server specified in the database name entered above (the database you created for LiveCycle Policy Server 7.x).

    Password: The password for the user account specified for the database name you entered above.

    JDBC driver: The location of the JDBC driver used with the LiveCycle Policy Server 7.x database. The driver may be located in the *[livecycle7_root]*/configurationManager/lib directory. You can also use the drivers in *[LiveCycleES root]*/lib/db<*database*>. Specifying the drivers here allows LiveCycle Configuration Manager to test the database connection.

22. Click **Test Connection** to ensure that the information here is valid and LiveCycle Configuration Manager can connect to the database, and then click **Next** to continue

23. On the LiveCycle Server Information screen, do the following tasks:
    - In the **LiveCycle ES User ID** box, type `administrator` if the box is not already populated.
    - In the **Password** box, type `password`.
    - Select **LiveCycle 7.x host is also the LiveCycle ES host** if the application server for LiveCycle ES is installed on the same computer as the LiveCycle 7.x server. If the previous and new application servers are installed on separate computers, do not select this option.
    - Provide the JNDI information for LiveCycle ES and LiveCycle 7.x. This information enables LiveCycle Configuration Manager to connect to the LiveCycle ES server and set preferences. Press **F1** for more information about the contents required for each field.
    - Provide the path to the Local Application Server Root directory. (For example, the default path is C:\Program Files\IBM\WebSphere\AppServer (Windows), /opt/IBM/WebSphere/AppServer (Linux and Solaris) and /usr/IBM/WebSphere/AppServer (AIX).

Caution: After completing the upgrade, you should change the default password in LiveCycle Administration Console. (See "Accessing LiveCycle Administration Console" on page 53.)

24. On the Upgrade Servers screen, click **Next**. This screen is for information purpose. If your LiveCycle 7.x server and LiveCycle ES server are on the same computer, prepare to stop the LiveCycle 7.x server so that you can start the application server on which LiveCycle ES will be deployed, and then configure it, beginning on the next screen.

25. On the Stop LiveCycle 7.x screen, you must stop the LiveCycle 7.x server if the target application server for LiveCycle ES is installed on the same computer.

    Note: Now you can start the application server on which LiveCycle ES will be deployed. If you have not done so already, you must configure the application server according to the instructions in the "Configuring WebSphere Application Server" section of *Preparing to Upgrade to LiveCycle ES* at http://www.adobe.com/go/learn_lc_upgradePreparation. Do not exit LiveCycle Configuration Manager. (If you do exit LiveCycle Configuration Manager, the information you have provided to this point is saved. You can restart LiveCycle Configuration Manager and quickly return to the same place after you have configured the application server.)

    When you have completed configuring application server for LiveCycle ES EAR, return to LiveCycle Configuration Manager and click **Next**.

26. On the Application Server Configuration Details screen, provide the information for the fields (mandatory fields are denoted by an asterisk) and then click Test Server Connection. When the test has completed successfully, click **Next**. Press **F1** for details about the required information.

27. On the Application Server Configuration Selection screen, select the check boxes to configure the application server and then click **Next**. Press **F1** for details about the required information.

28. On the Server Settings Configuration screen, provide the information for the fields, and then click **Next**. Press **F1** for details about the required information.

29. On the Datasource Configuration screen, provide the information for the fields and then click **Next**. Press **F1** for details about the required information.

30. On the Application Server Configuration screen, click **Configure**. Restart the server if you are prompted to do so. When the process has completed, click **Next**.

31. On the Application Server Configuration Validation screen, click **Validate**. When the process has completed, click **Next**.

32. On the Deploy LiveCycle ES EARs screen, click **Deploy**. This operation may take several minutes to complete. When the deployment has completed successfully, click **Next**.

33. On the LiveCycle ES Database Initialization screen, verify the host and port information, and then click **Initialize**. The database initialization task creates tables in the database, adds default data to the tables, and creates basic roles in the database. When the initialization has completed successfully, click **Next**.

34. ***(LiveCycle Business Activity Monitoring ES only)*** On the Initialize Business Activity Monitoring screen, provide the information for the following fields:

    Database type: The database on which BAM metadata is running.

    BAM Host: The name or IP address of the computer that hosts the application server on which BAM server is running.

    BAM HTTP Port: The HTTP service port that the database uses (for example, 9080).

    BAM Administrator User ID: The administrator ID required to log in to BAM Workbench. The default user ID is "system".

    BAM Administrator Password: The password to log in to the BAM Workbench. The default password is "manager".

35. Click **Initialize** to begin the initialization process. When initialization is complete, you can click **Next** to continue.

36. On the LiveCycle ES Server Information screen, click **Test Server Connection** to ensure that the information for the default application server is correct. When the test has completed successfully, click **Next**.

    Note: The server information that appears on this screen represents default values for the deployment. You can change the values if the LiveCycle 7.x server uses a different port.

    Testing the server connection helps to narrow troubleshooting in case failures occur in the deployment or validation. If the connection test passes, but deployment or validation fails in the next few steps, connectivity issues can be eliminated from the troubleshooting process.

37. On the LiveCycle Component Deployment screen, click **Deploy**. The components deployed at this time are Java archive files that plug into the LiveCycle ES service container for purposes of deploying, orchestrating, and executing services. When the deployment has completed successfully, click **Next**.

38. On the LiveCycle Component Deployment Validation screen, click **Validate**.
    LiveCycle Configuration Manager validates that the LiveCycle components (Java archive files) are deployed to and running on the LiveCycle ES server. When the validation has completed successfully, click **Next**.

39. ***(LiveCycle Document Security upgrade only)*** On the Unlock Credential Files Used By LiveCycle 7.x screen, select the credential that you want to import, and then type and confirm the password for the certificate file. Click **Next** to import the credentials and continue.

    Note: PFX files contain multiple credentials. In this version of LiveCycle ES, only PFX files containing one credential can be migrated.

    For information about migrating HSM-based credentials, see *Preparing to Upgrade to LiveCycle ES* at http://www.adobe.com/go/learn_lc_upgradePreparation.

40. On the Migrate Data Essential to LiveCycle ES Operation screen, click **Start**. When the migration is complete, click **Next**.

    This step involves copying LiveCycle Policy Server policies, configuration settings, forms, form data, preferences, FileType settings, job options, security settings, watched folders and email job sources (depending on the product or products you are upgrading), custom fonts and documents in the global document storage directory. For LiveCycle Policy Server, policies, external users, document licenses, watermarks, and revocation information are copied, and the user directory is synchronized.

41. On the LiveCycle ES Ready for Essential Tasks screen, click **Next**. The LiveCycle ES server is running on the application server and can process basic requests.

42. ***(LiveCycle Reader Extensions ES only)*** On the LiveCycle Reader Extensions ES Credential Configuration screen, specify the details associated with the Rights credential that activates the solution component services:

    LiveCycle Reader Extensions ES Rights credential: The path and file name of the Rights credential (.pfx or .p12 file type).

    LiveCycle Reader Extensions ES Rights credential password: The password associated with the credential. This password was provided with the credential file.

Name for the configured Rights Credential: The name (or alias) that LiveCycle Configuration Manager gives the credential when it is configured. If you are installing Reader Extensions ES for the first time, this can be any name. If you are upgrading from LiveCycle Reader Extensions, you must use the name of your LiveCycle 7.x Rights credential for LiveCycle ES. If you use a different name, you will have to modify code in existing custom applications or, in future LiveCycle ES, your existing LiveCycle QPACs.

This name appears in the Reader Extensions ES web interface, as well as the alias used to reference the credential through SDK calls. You can create any unique name for the Rights credential.

Tip: You can skip this step at this time by selecting **Configure later using LiveCycle Administration Console**. You can configure the Rights credential by using LiveCycle Administration Console after you complete the deployment. (After logging in to LiveCycle Administration Console, click **Home** > **Settings** >**Trust Store Management** > **Local Credentials**.)

Click **Configure** and then click **Complete**.

43. ***(LiveCycle Policy Server upgrade only)*** On the Migrate Remaining Data screen, click **Start** to begin migrating the remaining data from LiveCycle 7.x to LiveCycle ES. This screen appears only if you selected **Migrate Remaining Data** on the Upgrade Selection screen.

    This step migrates data and collateral that is not required to be in place in order for LiveCycle ES to run and accept user requests. For example, audit data used by LiveCycle Policy Server and Rights Management ES is not required to correctly grant and deny document viewing requests. Although it is important to migrate this data, it is not necessary to do so prior to making the LiveCycle ES server available to users. Records and data are available for viewing using LiveCycle Administration Console as they are migrated.

44. On the LiveCycle ES Samples Import screen, click **Import**. When the import has completed successfully, click **Next**.

45. On the Summary page, click **Exit**.

Manually deploying the EAR files

If you did not select Deploy LiveCycle ES EARs on the task selection screen, you must manually deploy them before you complete the upgrade. The EAR files must already be configured using LiveCycle Configuration Manager.

During the deployment process, you must deploy the following EAR files:

- adobe-livecycle-nativewebsphere-*[OS]*.ear
- adobe-livecycle-websphere.ear
- adobe-workspace-client.ear (only if you upgraded LiveCycle Form Manager to LiveCycle Workspace ES by installing LiveCycle Process Management ES)

Note: If you are upgrading Business Activity Monitoring ES, see "Upgrading to LiveCycle Business Activity Monitoring ES" on page 55 before you deploy the CAS_Adobe.ear file.

After you configure LiveCycle ES with LiveCycle Configuration Manager (required), these files are located in the following directory: *[LiveCycleES root]*/configurationManager/export/

You deploy LiveCycle ES solution components to WebSphere Application Server by deploying the component EAR files to the application server using WebSphere Administrative Console.

Before you deploy to WebSphere Application Server, you must start the application server on your computer. After deploying the required components, you must stop and restart the application server before starting any services.

You must run LiveCycle Configuration Manager to initialize the database, and deploy the components and LiveCycle ES archive files (LCAs). You can also choose to validate the components and LCA deployment.

➤ **To deploy the EAR files:**

1. In the WebSphere Administrative Console navigation tree, click **Applications** > **Install New Application**.
2. In the right pane, select **Remote file system**.
3. Click **Browse** and browse to one of the EAR files listed above, select it, and then click **OK**.
4. Select **Show me all installation options and parameters,** and then click **Next**.
5. Select **Generate Default Bindings** and click **Next**.
6. Select the last step in the left column of the right pane titled **Summary** and click **Finish**.
7. When the EAR file has installed successfully, in the **Messages** box, click **Save directly to Master Configuration**.
8. Repeat these steps for each of the EAR files listed above.

➤ **To start an application in WebSphere:**

1. In the WebSphere Administrative Console navigation tree, click **Applications** > **Enterprise Applications**.
2. Select any or all of the LiveCycle ES applications you want to start.
3. Click **Start**. The red "X" beside the status of each application changes to a green arrow, indicating that the application is running.

Uninstalling EAR files

If you need to redeploy a LiveCycle ES solution component, you must first uninstall the LiveCycle ES-related applications from the application server.

For example, if you have assembled LiveCycle ES solution components again to configure solution component properties differently, and the previous adobe-livecycle-websphere.ear file is already deployed, you must uninstall it before you deploy the newly assembled EAR files.

➤ **To uninstall the ear files:**

1. Start the application server.
2. Start WebSphere Administrative Console by typing `http://hostname:port/admin` in the URL line of a web browser.
3. In the navigation tree, click **Applications** > **Enterprise Applications**.

4. Select the adobe-livecycle-native-websphere-*[OS]*.ear, adobe-livecycle-websphere.ear, and adobe-workspace-client.ear applications, as well as any other installed LiveCycle ES applications, and then click **Stop**.

   Note: The adobe-workspace-client.ear is only deployed with LiveCycle Process Management ES.

5. Select the adobe-livecycle-native-websphere-*[OS]*.ear, adobe-livecycle-websphere.ear, and adobe-workspace-client.ear applications, as well as any other installed LiveCycle ES applications, and then click **Uninstall**.

6. Save your changes to the Master Configuration and restart WebSphere.

After uninstalling the EAR file, you may need to reconfigure your EAR file and redeploy, if you have added something that requires additional JVM or JMS settings. You should also run LiveCycle Configuration Manager to migrate essential and non-essential data, to reinitialize the database, and to deploy LiveCycle ES components.)

Next steps

If you used LiveCycle Configuration Manager to configure and deploy LiveCycle ES, you can now do the following tasks:

- Verify the deployment. (See "Verifying the deployment and accessing LiveCycle Administration Console" on page 53.)
- Access LiveCycle Administration Console. (See "Accessing LiveCycle Administration Console" on page 53.)
- Upgrading Business Activity Monitoring ES (See "Upgrading to LiveCycle Business Activity Monitoring ES" on page 55.)
- Migrate HSM credentials (for LiveCycle Document Security upgrades). (See "Migrating HSM credentials" on page 58.)
- Configure LiveCycle solution components to access LDAP. (See "Configuring LiveCycle ES to access LDAP" on page 60.)
- Configuring the LiveCycle ES Connectors for ECM systems. (See "Configuring the Connector for EMC Documentum service" on page 61 or "Configuring the Connector for IBM FileNet service" on page 64
- Set environment variables for PDF Generator ES. (See "Setting environment variables for PDF Generator ES" on page 67.)
- Update LiveCycle 7.x applications to ensure LiveCycle ES compatibility. (See "Updating client applications" on page 10.)
- Find out about some updates regarding upgrading from LiveCycle 7.x to LiveCycle ES. (See "Additional upgrade issues" on page 74.)
- Uninstall LiveCycle ES. (See "Uninstalling LiveCycle ES" on page 69.)

5 Post-Deployment Activities

This chapter describes how to verify the deployment by accessing LiveCycle Administration Console and checking the application server log files. It also describes how to get started using LiveCycle ES solution components and services after they are installed, configured, and deployed to your application server:

- "Verifying the deployment and accessing LiveCycle Administration Console" on page 53
- "Accessing solution component web applications" on page 57
- "Accessing User Management" on page 56
- "Configuring LiveCycle ES to access LDAP" on page 60
- "Setting environment variables for PDF Generator ES" on page 67

After you configure the settings in this chapter, see *Administering LiveCycle ES* at http://www.adobe.com/go/learn_lc_administration for additional information about configuring your LiveCycle ES environment for development and production.

Verifying the deployment and accessing LiveCycle Administration Console

You can verify the deployment by logging in to LiveCycle Administration Console. If you can log in, LiveCycle ES is running on the application server, and the default user has been created in the database.

You can review the application server log files to ensure that components were deployed correctly or to determine the cause of any deployment issues you may encounter.

Accessing LiveCycle Administration Console

LiveCycle Administration Console is the web-based portal for accessing a variety of configuration pages that let you set run-time properties that control the way LiveCycle ES operates. When you log in to LiveCycle Administration Console, you can access User Management, Archive Administration, and administrative configuration options for other services. LiveCycle Administration Console also provides access to Archive Administration, which administrators use for managing archives and deploying services to a production environment.

The default user name and password for logging in to LiveCycle Administration Console is *administrator* and *password*. After you log in the first time, access User Management and change the password.

Before you access LiveCycle Administration Console, LiveCycle ES must be deployed and running on your application server.

For information about using LiveCycle Administration Console, see *Archive Administration Help* (available from the Help menu on the LiveCycle Administration Console Home page).

➤ **To access LiveCycle Administration Console:**

1. Type the following URL in a web browser:

   `http://[host name]:[port]/adminui`

   The default port number for WebSphere is 9080.

   Note: Administrative users created in LiveCycle Policy Server 7.x are not migrated to LiveCycle ES during the upgrade. The super administrator password is reverted to the default value of *password* if it was changed in the LiveCycle Policy Server 7.x deployment. All policies created by different administrators in LiveCycle Policy Server 7.x are placed in the APS7 organizational policy set in LiveCycle ES. Events associated with LiveCycle 7.x administrators are not searchable by user name, but the original owner name is displayed.

2. In the **User Name** box, type `administrator` and, in the **Password** field box, type `password`.

3. After logging in, you can click **Services** to access the service administration pages or **Settings** to access the pages on which you can administer settings for different solution components.

Viewing the log files

Events, such as run-time or startup errors, are recorded to the application server log files. If you have problems deploying to the application server, you can use the log files to help you find the problem. You can open the log files using any text editor.

The following log files are in the *[appserver root]*/profiles/default/logs/*servername* directory:

- SystemErr.log
- SystemOut.log
- StartServer.log

Deleting working files that contain sensitive data

During upgrade, all the information is extracted from the LiveCycle Policy Server database and written to working files, from which the information is then migrated into the LiveCycle ES database. The files containing this information remain in the *[LiveCycleES root]*/configurationManager/working/upgrade directory after the data migration is complete.

Some of this data is sensitive information, such as passwords and document encryption keys. After you verify that the upgrade is complete (essential and non-essential data is migrated) and Rights Management ES is working as expected, you must delete the LiveCycle Policy Server migration files.

In the *[LiveCycleES root]*/configurationManager/working/upgrade, directory, delete all the files whose names begin with OrigExported and Intermediate. Approximately 50 files need to be removed. Do not delete the sharedData file.

Configuring Acrobat 8.1 for PDF Generator ES

Note: This functionality is supported only on the Windows platform.

If you did not choose to install Acrobat 8.1 using the LiveCycle ES installer, you need to complete the following procedure to set up Acrobat 8.1 for use with PDF Generator ES.

➤ **To configure Acrobat 8.1 for use with PDF Generator ES:**

1. If a previous version (8.0 or earlier) of Acrobat is installed, uninstall it using **Add or Remove Programs** in the Windows Control Panel.
2. Navigate to one of the following folders on the LiveCycle ES installation media:
   - additional\acrobat\efg\
   - additional\acrobat\jpn\
3. Install Acrobat 8.1 by running the AutoPlay.exe file.
4. Navigate to the additional\scripts folder on the LiveCycle ES installation media.
5. Run the following batch file:

   `Acrobat_for_PDFG_Configuration.bat` *`[LiveCycleES root]`*

➤ **To validate the Acrobat 8.1 installation:**

1. Navigate to a PDF file on your system and double-click it to open it in Acrobat.
2. If the PDF file opens successfully, Acrobat 8.1 is installed correctly. If the PDF fails to open correctly, uninstall Acrobat and reinstall it.

Note: Ensure that you dismiss all the Acrobat dialog boxes that are displayed after Acrobat installation is complete and disable the automatic updates for Acrobat.

Set the environment variable, `Acrobat_PATH` to point to Acrobat.exe (for example, C:\Program Files\Adobe\Acrobat 8.0\Acrobat\Acrobat.exe).

Final setup for LiveCycle Rights Management ES

LiveCycle Rights Management ES requires the application server to be configured to use SSL. For the configuration instructions, see *Administering LiveCycle ES* at help.adobe.com/en_US/livecycle/es/admin_guide.pdf.

Upgrading to LiveCycle Business Activity Monitoring ES

Upgrading from LiveCycle Business Activity Monitor 7.x to LiveCycle Business Activity Monitoring ES is performed separately from the main LiveCycle upgrade. You must undeploy and uninstall LiveCycle Business Activity Monitor 7.x and then configure and deploy BAM Server. The instructions for configuring and deploying BAM Server are located in the *Installing and Deploying LiveCycle ES* document for your application server:

Installing and deploying LiveCycle ES for WebSphere at www.adobe.com/go/learn_lc_installWebSphere

➤ **To undeploy and uninstall Business Activity Monitor 7.x:**

1. Stop and undeploy the LiveCycle 7.x version of the BAM Server EAR file from the application server.
2. Delete all the BAM logs and delete all the files from the recovery log directory that have names similar to the following patterns:
   - filestore*.dat
   - DEFAULTRECOVERYLOGGER_*
   - chkpoint*
   - delete the chkpoint* files under *[appserver_root]*/profiles/*[BAM Profile]* if it exists
3. If you plan to use the same database for the new BAM Server metadata database, drop all the tables and views from the current BAM Server metadata database.
4. Configure and deploy BAM Server for LiveCycle ES by following all the instructions in the "Manually Configuring BAM Server for LiveCycle ES" section in the *Installing and Deploying LiveCycle ES* document for your application server.

Accessing User Management

User Management allows administrators to maintain a database of all users and groups, synchronized with one or more third-party user directories. User Management provides authentication, authorization, and user management for LiveCycle ES solution components, including Reader Extensions ES, Workspace ES, Rights Management ES, Process Management ES, and Forms ES.

Note: User roles created in LiveCycle 7.x are migrated to LiveCycle ES, but cannot be modified or deleted.

Passwords in LiveCycle ES must contain at least 8 characters. For user records migrated from LiveCycle 7.x, LiveCycle ES does not enforce this length while fetching and displaying the user record. However, if you change a user record and save it, you are prompted to change the password to contain 8 characters or more.

➤ **To access User Management:**

1. Log in to LiveCycle Administration Console.
2. On the Home page of LiveCycle Administration Console, click **Settings**.
3. On the Settings page, click **User Management**.

Note: For information about configuring users with User Management, click **User Management Help** in the upper-right corner of the User Management page.

Accessing solution component web applications

After LiveCycle ES is deployed, you can access the web applications associated with the following solution components:

- LiveCycle Reader Extensions ES
- LiveCycle Workspace ES
- LiveCycle Rights Management ES

After accessing the web applications using the default administrator permissions to ensure that they are accessible, you can create additional users and roles so that others can log in and use the applications. For information, see the User Management Help, accessible through the LiveCycle Administration Console. After you have changed the administrator user name and password, the default values are no longer valid.

You can find out more about how to use these applications by accessing the Help available within each application.

➤ **To access the Reader Extensions ES web application:**

1. Open a web browser and enter this URL:

   http://localhost:9080/ReaderExtensions (local deployment using the default port)

2. Log in using the default user name and password:

   User name: administrator

   Password: password

Note: You must have administrator or super user privileges to log in using the default user name and password. To allow other users to access the Reader Extensions ES web application, you must create the user accounts in User Management and grant them the Reader Extensions Web Application role.

➤ **To access Workspace ES:**

1. Open a web browser and enter this URL:

   http://localhost:9080/workspace (local deployment using the default port)

2. Log in using the default user name and password:

   User name: administrator

   Password: password

Accessing LiveCycle Rights Management ES

To log in to Rights Management ES end user application, you must be assigned the LiveCycle Rights Management End User role. All new and existing users are not granted this role by default. You must assign a user account with the LiveCycle Rights Management End User role in User Management and then log in to Rights Management ES by using the login information associated with the user that you create.

Note: LiveCycle Policy Server 7.x administrative user accounts that are created in User Management are not migrated to the LiveCycle ES database during the upgrade.

For information about setting up users and roles for Rights Management ES, see *Administering LiveCycle ES* at http://www.adobe.com/go/learn_lc_administration.

The Rights Management ES end-user web application is then accessible from this URL:

http://*[server]*:*[port]*/edc/Main.do

The Rights Management ES administration web application is accessible from this URL:

http://*[server]*:*[port]*/adminui

Note: You may need to restart the application server if you cannot log in as a user other than administrator.

When a user adds a principal user to a policy entry in Rights Management ES, by default no principal users are visible because the My Policies policy set does not include a domain. To add visible users and groups, you can change the My Policies configuration in the Rights Management ES administration web application to add a domain. All the users in the added domain(s) are visible and can be added to a user policy. For information, see "Editing Policy Sets" in *Rights Management ES Help at* http://www.adobe.com/go/learn_lc_adminRightsMgmt.

➤ **To assign the LiveCycle Rights Management End User role:**

1. Log in to LiveCycle Administration Console. (See "Accessing LiveCycle Administration Console" on page 53.)
2. Click **Settings** > **User Management** > **Users and Groups**.
3. In the **Find** box, type `all`.
4. In the **In** list, select **Groups**, and then click **Find**.
5. Click **All Principals** for the required domain(s).
6. On the **Role Assignments** tab, click **Find Roles**.
7. Select **LiveCycle Rights Management End Users** from the list and click **OK**.
8. Click **Save**.

Migrating HSM credentials

If you are using an Hardware Security Module (HSM) device to store credentials for LiveCycle Document Security 7.x, information about the credentials stored in the device must be migrated to the LiveCycle ES trust store.

The function of signing documents that was provided by LiveCycle Document Security 7.x is provided in LiveCycle ES by the Signature service (included in the Digital Signatures ES solution component). The LiveCycle ES Trust Store stores the various parameters that the Signature service requires for HSM signing, including options for SHA1 and certificate-based identification of an HSM signing key.

Upgrading LiveCycle Document Security 7.x to Digital Signatures ES includes migrating information from the trust.xml file, which is not used by LiveCycle ES, to the Trust Store. Migrated data includes file-based credentials, certificates, and CRLs and preferences information. This process is performed by

LiveCycle Configuration Manager. However, only file-based credentials are migrated, specifically the "p12record" tag in trust.xml. The HSM reference credentials in the "hsmrecord" tag are not migrated. You must manually migrate HSM credentials.

For more information about Trust Store and credentials used with Digital Signatures ES, log in to LiveCycle Administration Console, browse to Settings > Trust Store Management, and click Help.

➤ **To migrate HSM credentials:**

1. Log in to LiveCycle Administration Console.
2. Click **Settings** > **Trust Store Management** > **HSM Credentials**.
3. Click **Add** to add a credential to the LiveCycle ES Trust Store. For detailed information, click **Help** and go to the "Managing HSM Credentials" section.
4. Add all the HSM credentials that you used with LiveCycle 7.x.

Enabling FIPS mode

LiveCycle ES provides a FIPS mode to restrict data protection to Federal Information Processing Standard (FIPS) 140-2 approved algorithms using the RSA BSAFE Crypto-C 2.1 encryption module.

If you did not enable this option with LiveCycle Configuration Manager during the LiveCycle ES configuration or if you enable it but want to turn it off, you can change this setting through the LiveCycle Administration Console.

Modifying FIPS mode requires you to restart the server.

FIPS mode does not support Acrobat versions earlier than 7.0. If FIPS mode is enabled and the processes Encrypt With Password and Remove Password include the Acrobat setting Acrobat 5, the process fails.

In general, when FIPS is enabled, the Assembler service will not apply password encryption to any document. If this is attempted, a FIPSModeException is thrown indicating that "Password encryption is not permitted in FIPS mode." Additionally, the`PDFsFromBookmarks` element is not supported in FIPS mode when the base document is password-encrypted.

➤ **To turn FIPS mode on or off:**

1. Log in to the LiveCycle Administration Console.
2. Browse to **Settings** > **Core System** > **Core Configurations > Configurations**.
3. Select the **Enable FIPS** option to enable FIPS mode or deselect it to disable FIPS mode.
4. Click **OK**.
5. Restart the application server.

Note: LiveCycle software does not validate code to ensure FIPS compatibility. It provides a FIPS operation mode so that FIPS-approved algorithms are used for cryptographic services from the FIPS-approved libraries (RSA).

Configuring LiveCycle ES to access LDAP

If you configured LDAP for LiveCycle 7.x products, those settings are migrated during the upgrade process, and you do not need to perform the steps in this section. If you did not previously configure LDAP, you can use the following procedure as a guideline when configuring User Management to support authentication using LDAP.

➤ **To configure User Management with LDAP:**

1. Open a web browser, navigate to `http://[host name]:[port]/adminui` and log in. (See "Accessing LiveCycle Administration Console" on page 53.)
2. Click **Settings** > **User Management** > **Domain Management** and click **New Enterprise Domain** or **New Local Domain**.
3. In the **ID** box, type a unique identifier for the domain.
4. In the **Name** box, type a descriptive name for the domain.
5. Click **Add Authentication** and, in the Authentication Provider list, select **LDAP**.
6. Click **OK**.
7. Click **Add Directory**.
8. Under Populate Page With, select a directory settings option such as **Default Sun ONE values**.
9. Specify values in the **Server**, **Port**, **SSL**, and **Binding** boxes as required. For details on the settings, see "Directory settings" in *User Management Help*.
10. Configure the user settings and group settings as required. For details on the settings, see "Directory settings" in *User Management Help*.
11. (Optional) Test your configuration:
    - Click **Test**.
    - On the Test Directory pane, in the **Find** box, enter an object name and, in the **using** box, select the object's type, such as **Login ID**.
    - Click **Test**. If successful, your object's details are displayed, and then click **Back**.
12. Click **OK** to exit the Add Directory page, and click **OK** again to exit.

Configuring HTML digital signature

To use the HTML digital signature feature of LiveCycle Forms ES, you must complete the following procedure.

➤ **To enable HTML digital signature:**

1. Manually deploy the *[LivecycleES root]*/deploy/adobe-forms-ds.ear file to your application server.
2. Log in to LiveCycle Administration Console.
3. Click **Services** > **LiveCycle Forms ES**.
4. Select **HTML Digital Signature Enabled**.

Configuring the Connector for EMC Documentum service

If you installed the Connector for EMC Documentum service as part of your LiveCycle ES solution, complete the following procedure to configure the service to connect to the Documentum repository.

➤ **To configure Connector for EMC Documentum:**

1. Locate the `adobe-component-ext.properties` file in the *[WAS HOME]*/AppsServer/profiles/*[profile name]* folder. If the file does not exist, you must create it. Add a new system property that provides the location of the Documentum Content Server config folder and the following Documentum Foundation Classes JAR files:

   - dfc.jar
   - dfcbase.jar

   The new system property should take this form:

   ```
   [component id]_[component version].ext=[JAR files and/or folders]
   ```

   For example, using default Content Server and Documentum Foundation Classes installations, you add the following system property on a new line, with no line breaks, and end the line with a carriage return, to the file:

   ```
   com.adobe.livecycle.ConnectorforEMCDocumentum_8.0.3174.1.156395.1.ext
   =C:/Documentum/Config,C:/Program Files/Documentum/Shared/dfc.jar,
   C:/Program Files/Documentum/Shared/dfcbase.jar
   ```

   You can determine the version of the component by logging in to the LiveCycle Administration Console and navigating to **Services** > **Archive Administration** > **Service Management**, and then searching for the component. The version number is listed in the **Component Version** column.

2. If WebSphere Application Server is not currently running, start the server. Otherwise, stop and then restart the server.

3. Open a web browser and enter this URL:

   http://localhost:9080/adminui (local deployment using the default port)

4. Log in using the default user name and password:

   User name: administrator

   Password: password

5. Navigate to **Services** > **LiveCycle ES Connector for EMC Documentum** > **Configuration Settings**.

6. Type all of the required Documentum repository information. To use Documentum as your repository provider, in the Repository Service Provider Information area, select **EMC Documentum Repository Provider**, and then click **Save**. For more information about the Documentum repository information, see *Documentum Administration Help* at www.adobe.com/go/learn_lc_adminDocumentum.

7. (Optional) Navigate to **Repository Credentials Settings**, click **Add**, specify the Docbase information, and then click **Save**. For more information about the Documentum repository information, see *Documentum Administration Help* at www.adobe.com/go/learn_lc_adminDocumentum.

8. Navigate to **Services** > **Archive Administration** > **Service Management**, select the following services, and then click **Start**:
   - EMCDocumentumAuthProviderService
   - EMCDocumentumContentRepositoryConnector
   - EMCDocumentumRepositoryProvider

   If any of the services do not start correctly, check the settings entered in step 6.

9. Do one of the following tasks:
   - To use the Documentum Authorization service (EMCDocumentumAuthProviderService) to display content from a Documentum repository in the Resources view of Workbench ES, continue with this procedure. Using the Documentum Authorization service overrides the default LiveCycle ES authorization and must be configured to log in to Workbench ES using Documentum credentials.
   - To use the LiveCycle ES repository, log in to Workbench ES using the LiveCycle ES super administrator credentials (by default, *Administrator* and *password*). You have now completed the required steps for this procedure. The credentials provided in step 6 are used for accessing the default repository in this case and use the default LiveCycle ES authorization service.

10. Restart WebSphere Application Server.

11. Log in to the LiveCycle Administration Console, navigate to **Settings** > **User Management** > **Domain Management**, and click **New Enterprise Domain**.

12. Type a domain ID and name. The domain ID is the unique identifier for the domain. The name is a descriptive name for the domain.

13. Add a custom authentication provider:
    - Click **Add Authentication**.
    - In the **Authentication Provider** list, select **Custom**, and select **EMCDocumentumAuthProvider**.
    - Click **OK**.

14. Add an LDAP authentication provider:
    - Click **Add Authentication**.
    - In the **Authentication Provider** list, select **LDAP**.
    - Click **OK**.

15. Add an LDAP directory:
    - Click **Add Directory**.
    - In the **Profile Name** box, type a unique name, and then click **Next**.
    - Specify values for the **Server**, **Port**, **SSL**, **Binding**, and **Populate page with** options. If you select **User** for the **Binding** option, you must also specify values for the **Name** and **Password** fields. (Optional) Select **Retrieve Base DN** to retrieve base domain names, as required. When finished, click **Next**.

      For details about the settings, see *User Management Help* at www.adobe.com/go/learn_lc_adminUM.
    - Configure the user settings, click **Next**, configure group settings, as required, and then click **Next**.

      For details about the settings, see *User Management Help* at www.adobe.com/go/learn_lc_adminUM.

16. Click **OK** to exit the Add Directory page, and click **OK** again.

17. Select the new enterprise domain and click **Sync Now**. Depending on the number of users and groups in your LDAP network and the speed on your connection, the synchronization process may take several minutes.

    To verify the status of the synchronization, click **Refresh** and view the status in the **Current Sync State** column.

18. Click **Settings** > **User Management** > **Users and Groups**.

19. Search for users that were synchronized from LDAP. Select one or more users, click **Assign Role**, select one or more LiveCycle ES roles, and then click **OK**. Click **OK** a second time to confirm the role assignment. Repeat this step for all users you assign roles to. For more information about assigning LiveCycle ES roles, see *User Management Help* at www.adobe.com/go/learn_lc_adminUM.

20. Start Workbench ES and log in using the following credentials:

    Username: *[username]@[repository_name]*

    Password: *[password]*

    The Documentum repository should now be visible in the Resources view within Workbench ES. If you do not log in using the *username@repository name*, Workbench ES attempts to log in to the default repository specified in step 6.

After you configure your Connector for EMC Documentum service, you should see *Administering LiveCycle ES* at www.adobe.com/go/learn_lc_administration for information on correctly configuring Workbench ES functions properly with your Documentum repository.

Creating the XDP MIME format in your Documentum repository

Before users can store and retrieve XDP files from a Documentum repository, you must do one of these tasks:

- Create a corresponding XDP format in each repository where users will access XDP files.
- Configure the Connector for EMC Documentum service to use a Documentum Administrator account when accessing the Documentum repository. In this case, the XDP format is created by the Connector for EMC Documentum service whenever it is required.

➤ **To create the XDP format on Documentum Content Server using Documentum Administrator:**

1. Log in to Documentum Administrator.

2. Click **Formats**.

3. Select **File** > **New** > **Format**.

4. Type the following information into the corresponding fields:

   Name: `xdp`

   Default File Extension: `xdp`

   Mime Type: `application/xdp`

5. Repeat steps 1 - 4 for all other Documentum repositories where users will store XDP files.

➤ **To configure the Connector for EMC Documentum service to use a Documentum Administrator:**

1. Open a web browser and enter this URL:

   http://localhost:9080/adminui (local deployment using the default port)

2. Log in using the default user name and password:

   User name: administrator

   Password: password

3. Click **Services** > **LiveCycle ES Connector for EMC Documentum** > **Configuration Settings**.

4. In the Documentum Principal Credentials Information area, update the following information and then click **Save**:

   User Name: *[Documentum Administrator user name]*

   Password: *[Documentum Administrator password]*

5. Click **Repository Credentials Settings**.

6. Select a repository from the list or, if none exist, click **Add**.

7. Type the following information:

   Repository Name: *[Repository Name]*

   Repository Credentials User Name: *[Documentum Administrator user name]*

   Repository Credentials Password: *[Documentum Administrator password]*

8. Click **Save**.

9. Repeat steps 7 - 9 for all repositories where users will store XDP files.

Configuring the Connector for IBM FileNet service

If you installed the Connector for IBM FileNet service as part of your LiveCycle ES solution, complete the following procedure to configure the service to connect to the FileNet object store.

➤ **To configure Connector for IBM FileNet:**

1. Locate the `adobe-component-ext.properties` file in the *[WAS HOME]*/AppsServer/profiles/*[profile name]* folder. If the file does not exist, you must create it. Add a new system property that provides the location of the following Application Engine JAR files:
   - activation.jar
   - javaapi.jar
   - log4j-1.2.8.jar
   - mailapi.jar
   - p8cjares.jar
   - soap.jar
   - xercesimpl.jar
   - xml-apis.jar

The new system property should take this form:

```
[component id]_[component version].ext=[JAR files and/or folders]
```

For example, using a default Application Engine installation, add the following system property on a new line, with no line breaks, and end the line with a carriage return, to the file:

```
com.adobe.livecycle.ConnectorforIBMFileNet_8.0.3174.1.156395.1.ext=
C:/Program Files/FileNet/lib2/activation.jar,
C:/Program Files/FileNet/lib2/javaapi.jar,
C:/Program Files/FileNet/lib2/log4j-1.2.8.jar,
C:/Program Files/FileNet/lib2/mailapi.jar,
C:/Program Files/FileNet/lib2/p8cjares.jar,
C:/Program Files/FileNet/lib2/soap.jar,
C:/Program Files/FileNet/lib2/xercesImpl.jar,
C:/Program Files/FileNet/lib2/xml-apis.jar
```

You can determine the version of the component by logging in to LiveCycle Administration Console and navigating to **Services** > **Archive Administration** > **Service Management**, and then searching for the component. The version number is listed in the **Component Version** column.

2. If WebSphere Application Server is not currently running, start the server. Otherwise, stop and then restart the server.

3. Open a web browser and enter this URL:

   http://localhost:9080/adminui (local deployment using the default port)

4. Log in using the default user name and password:

   User name: administrator

   Password: password

5. Navigate to **Services** > **LiveCycle ES Connector for IBM FileNet** > **Configuration Settings**.

6. Type all of the required FileNet repository information and, in the Repository Service Provider Information area, select **IBM FileNet Repository Provider**, and then click **Save**. For more information about the FileNet repository information, see *FileNet Administration Help* at http://www.adobe.com/go/learn_lc_adminFileNet.

   Note: The credentials you provide during this step are validated when the IBM FileNet repository services are started in the next step. If the credentials are invalid, an error is thrown and the services will fail to start.

7. Navigate to **Services** > **Archive Administration** > **Service Management**, click the following services, and then click **Start**:

   - IBMFileNetAuthProviderService
   - IBMFileNetContentRepositoryConnector
   - IBMFileNetRepositoryProvider

   If any of the services do not start correctly, check the settings entered in step 6.

8. Do one of the following tasks:
   - To use the FileNet Authorization service (IBMFileNetAuthProviderService) to display content from a FileNet object store in the Resources view of Workbench ES, continue with this procedure. Using the FileNet Authorization service overrides the default LiveCycle ES authorization and must be configured to log in to Workbench ES using FileNet credentials.
   - To use the LiveCycle ES repository, log in to Workbench ES using the LiveCycle ES super administrator credentials (by default, `Administrator` and `password`). You have now completed the required steps for this procedure. The credentials provided in step 6 use the default LiveCycle ES authorization service for accessing the default repository in this case.
9. Restart WebSphere Application Server.
10. Log in to the LiveCycle Administration Console, navigate to **Settings** > **User Management** > **Domain Management**, and click **New Enterprise Domain**.
11. Type a domain ID and name. The domain ID is the unique identifier for the domain. The name is a descriptive name for the domain.
12. Add a custom authentication provider:
    - Click **Add Authentication**.
    - In the **Authentication Provider** list, select **Custom**, and select **IBMFileNetAuthProviderService**.
    - Click **OK**.
13. Add an LDAP authentication provider:
    - Click **Add Authentication**.
    - In the **Authentication Provider** list, select **LDAP**.
    - Click **OK**.
14. Add an LDAP directory:
    - Click **Add Directory**.
    - In the **Profile Name** box, type a unique name, and then click **Next**.
    - Specify values for the **Server**, **Port**, **SSL**, **Binding**, and **Populate page with** options. If you select **User** for the **Binding** option, you must also specify values for the **Name** and **Password** fields. (Optional) Select **Retrieve Base DN** to retrieve base domain names, as required. When finished, click **Next**.

      For details about the settings, see *User Management Help* at http://www.adobe.com/go/learn_lc_adminUM.
    - Configure the user settings, click **Next**, configure group settings, as required, and then click **Next**.

      For details about the settings, see *User Management Help* at http://www.adobe.com/go/learn_lc_adminUM.
15. Click **OK** to exit the Add Directory page, and click **OK** again.
16. Select the new enterprise domain and click **Sync Now**. Depending on the number of users and groups in your LDAP network and the speed on your connection, the synchronization process may take several minutes.

    To verify the status of the synchronization, click **Refresh** and view the status in the **Current Sync State** column.
17. Click **Settings** > **User Management** > **Users and Groups**.

18. Search for users that were synchronized from LDAP. Select one or more users, click **Assign Role**, select one or more LiveCycle ES roles, and then click **OK**. Click **OK** a second time to confirm the role assignment. Repeat this step for all users you want to assign roles to. For more information about assigning LiveCycle ES roles, see *User Management Help* at http://www.adobe.com/go/learn_lc_adminUM.

19. Start Workbench ES and log in using the following credentials:

    Username: *[username]@[repository_name]*

    Password: *[password]*

    The FileNet object store should now be visible in the Resources view within Workbench ES. If you do not log in using the *username@repository name*, Workbench ES attempts to log in to the default repository specified in step 6.

After you configure your Connector for IBM FileNet service, you should see *Administering LiveCycle ES* at www.adobe.com/go/learn_lc_administration for information on correctly configuring Workbench ES functions properly with your FileNet repository.

Setting the Adobe PDF Printer as default for PDF Generator ES

You must set the Adobe PDF Printer as the default printer on the server. If the Adobe PDF Printer is not set as the default, PDF Generator ES cannot convert files successfully.

➤ **To set the default printer:**

1. Click **Start** > **Printers and Faxes**.

2. In the Printers and Faxes window, right-click **Adobe PDF** and select **Set as Default Printer**.

Setting environment variables for PDF Generator ES

You must manually set the environment variables if you installed the PDF Generator ES solution component and configured it to convert native application files (such as Microsoft Office documents) to PDF. You must set the following environment variables:

- `Acrobat_PATH`
- `Notepad_PATH`
- `Photoshop_PATH`
- `WordPerfect_PATH`
- `PageMaker_PATH`
- `FrameMaker_PATH`
- `OpenOffice_PATH`

The `OpenOffice PATH` variable must be set to the path to the folder where the OpenOffice executable is located (for example, C:\Program Files\OpenOffice.org 2.2).

All other `PATH` variables must be set to point to the executable associated with the application (for example, C:\Program Files\Adobe\FrameMaker7.2\FrameMaker.exe or C:\Program Files\Adobe\Acrobat 8.0\Acrobat\Acrobat.exe).

➤ **To set the PATH variables on Windows:**

1. Click **Start** and then right-click **My Computer** and click **Properties**.
2. In the System Properties dialog box, click the **Advanced** tab and click **Environment Variables**.
3. In the Environment Variables dialog box, click **New** and enter the following information:

   Variable name: Acrobat_PATH

   Variable value: C:\Program Files\Adobe\Acrobat 8.0\Acrobat\Acrobat.exe
4. Perform these steps for each variable in the list above (for the applications that you installed).

➤ **To set the PATH variables on Linux or UNIX (OpenOffice only):**

- Type the following command:

```
export OpenOffice_PATH /opt/openoffice.org2
```

Setting PDF Generator ES watched folder performance parameters

To avoid java.io.IOException error messages indicating that not enough disk space is available to perform PDF conversions using a watched folder, you can modify the settings for PDF Generator ES in LiveCycle Administration Console.

➤ **To set performance parameters for PDF Generator ES:**

1. Log in to LiveCycle Administration Console and click **Services** > **Archive Administration** > **Service Management**.
2. Click **Configure PDFGConfigService** and then set the following values:

   PDFG Cleanup Scan Seconds: 30 min

   Job Expiration Seconds: 100 min

Verifying that all languages are displayed after conversion with PDF Generator ES

When HTML files are converted to PDF using PDF Generator ES, some East Asian languages, such as Japanese, Korean, and Chinese, as well as left-to-right languages such as Arabic, Armenian, Georgian, Hebrew, Indic, Thai, and Vietnamese, may not be displayed in the PDF file.

To display these languages, appropriate fonts must be present on the client and server.

➤ **To verify that East Asian characters are displayed in Windows:**

1. Click **Start** > **Control Panel** > **Regional and Language Options**.
2. On the **Languages** tab, select **Install Files for East Asian Languages**.
3. On the **Advanced** tab, under Code Page Conversion Tables, select all the options.

If converted PDF files still have fonts missing, verify that the Arial Unicode MS (TrueType) font (ARIALUNI.TTF) is present in the C:\WINDOWS\Fonts directory.

Creating email endpoints for email notifications

After upgrading to LiveCycle ES from LiveCycle 7.x, you must create an email endpoint if you used email notifications with attachments in LiveCycle 7.x and want to ensure that users can continue to submit tasks by email. The email endpoint is created for the CompleteTask service.

➤ **To add an endpoint to the CompleteTask service:**

1. Log in to LiveCycle Administration Console and click **Services** > **Archive Administration** > **Service Management**.
2. Click the **CompleteTask** service in the list of services.
3. Click the **End Points** tab, select **Email** from the list, and then click **Add**.
4. Set the options on the Add Email Endpoint screen, and then click **Add**.

For more information about the attributes you can set for an Email endpoint, see the section "Endpoint attributes" in the *Archive Administration Help.*

Uninstalling LiveCycle ES

The uninstall program in the *[LivecycleES root]* directory does not remove any files that you deployed to your application server. You must manually undeploy these applications.

Caution: By running the uninstall program, all of the contents within the product installation directory are subject to removal without further warning. Before you proceed, back up any data you do not want to lose.

➤ **To remove the files from your computer:**

1. Navigate to the *[LivecycleES root]*/_uninst/server directory and start the uninstall program:
   - (Windows) Double-click the livecycle8_uninstall.exe file. Alternatively, you can use the Add or Remove Programs function in the Control Panel.
   - (Linux, UNIX) From a command prompt, type ./`livecycle8_uninstall.sh`
2. Follow the on-screen instructions in the uninstall program and then click **Finish**.

A Troubleshooting

This section discusses possible issues you may encounter when installing and deploying LiveCycle ES, and some suggested steps for avoiding them or working around them.

Getting help

This section describes the steps you should take before you contact Adobe Support. If, after reviewing the LiveCycle ES documentation, you have not resolved your issues, contact Adobe Support. To help expedite your service, have the following information available:

- What were you doing when the problem occurred?
- Can you repeat the problem?
- Did you see any error message when the problem occurred? Did you see anything else?
- If you disable the Show friendly HTTP error messages' options in Internet Explorer (Tools > Internet Options > Advanced), do the errors persist?

Installation considerations

If you are having problems installing, configuring, or deploying LiveCycle ES, ensure that you have carefully followed the instructions in these LiveCycle ES documents:

- *Preparing to Upgrade to LiveCycle ES* at http://www.adobe.com/go/learn_lc_upgradePreparation
- *Upgrading to LiveCycle ES* for your application server (this document)
- *Administering LiveCycle ES* at http://www.adobe.com/go/learn_lc_administration

If you have installed and configured everything according to the documentation, review the following sections for issues similar to those you are encountering.

Application server considerations

Check the following application server settings before you contact Adobe Support:

Initial heap size: 512 Mb

Maximum heap size: 1024 Mb

Prepared statement cache: 100

Database connection pool maximum: 50

Topics and queues connection factories:

- **Session pool maximum connections**: 30
- **Connection pool maximum connections**: 30

Database initialization considerations

If you are having problems initializing the LiveCycle ES server, consider the following possibilities:

- Database instances must contain only alphanumeric characters in their names.
- (Linux and UNIX) Database instances must not exceed the platform-specific threshold of 8 characters.
- For upgrading to LiveCycle ES, a default schema is associated with each database user. When LiveCycle ES initializes using a database user, the data is populated in the default schema of the user. During upgrade, you must use same user that was used for LiveCycle 7.x. This applies to Oracle, DB2, and SQL Server.

If the initialization fails at the beginning of the process, verify that the following tasks are done:

- (Non-turnkey install) The LiveCycle ES database is created and the user has full access rights to it.
- The database server is accessible when you ping it.
- The database is empty; that is, it has no tables, sequences, views, or index tables.
- The JNDI name for `IDP_DS` is created.

If initialization fails while writing to the Registry, check the application server logs for errors that pertain to the queues and topics. If errors exist, verify that the queues and topics are configured properly.

Troubleshooting with log files

LCM log file

By default, the LCM log file is located in *[LiveCycleES root]*configurationManger\log and will be named *lcm.0.log* (or a similar name). The log files are useful for LiveCycle Configuration Manager failure analysis and may be required when dealing with Adobe Enterprise Support.

Viewing the JVM system output and error logs

The JVM system output and error logs are valuable tools for troubleshooting problems with your server.

➤ **To view the JVM system output and error logs:**

1. Log in to WebSphere Administrative Console.
2. In the navigation tree, click **Troubleshooting** > **Logs and Trace**, and then click the name of the application server.
3. Click **JVM Logs**.
4. Click the **Runtime** tab and click **View** under either System.out (to view the JVM system output log) or System.err (to view the error log). If any of the selections are unavailable, you can view them from the **Configuration** tab by specifying the System.out and System.err file names. By default, the files are in the following location:

   [appserver root]/profiles/*[profile_name]*/logs/*[server_name]*

Modifying WebSphere log level

You must modify your WebSphere log level to filter out multiple "Deprecated usage of direct JNDI lookup of resource IDP_DS" messages written to the log file. You can modify SystemOut.log to remove these messages by setting the log level as follows:

```
*=info:com.ibm.ejs.j2c.ConnectionFactoryBuilderImpl=severe.
```

Refer to your IBM WebSphere documentation for specific information on setting log levels.

Error messages

This section contains a list of error messages and description that are specific to LiveCycle ES.

Class not found

If you see this error message, check whether any of these problems exist:

- The class path setting is invalid or missing.
- The JAR file is obsolete.
- A compilation problem exists in the class.

JNDI name not found

If you see this error message and if the symptom is an exception stack trace showing the following line of code, check whether the expected name is spelled incorrectly. If the name in incorrect, you must fix the code:

```
javax.naming.NameNotFoundException: jdbc/<badName>
```

➤ **To correct the most common JNDI exceptions:**

1. Check the JNDI tree on the LiveCycle ES application server to determine whether the name used appears in the tree:
   - If yes, it is most likely that your code has not properly set up the `InitialContext` object being used for the look-up, and the look-up is being done on a JNDI tree that is not the one that the resource is listed in. Refer to the property values to use in the *Installing and Deploying* document for your application server.
   - If no, continue to step 2.
2. Check whether the resource appears in the JNDI tree under a name other than that listed in the look-up:
   - If yes, you are using the incorrect look-up name; you must provide the correct name.
   - If no, continue to step 3.

3. Review the application server logs during startup. If the application server is configured to make this resource available but something is not working properly, an exception will be shown here. Verify whether an exception is shown:
   - If yes, review the exception and stack trace. If the NameNotFoundException is a symptom of another problem based on your investigation of the server logs, move on to the troubleshooting steps for that problem.
   - If the resource is not listed in the JNDI tree, and there is no exception at startup to explain why it is not available, continue to step 4. The most probable issue is that the application server is not configured properly to make that resource available.
4. Review the application server configuration to find out whether it is configured to make this resource available:
   - If no, see "Manually Configuring WebSphere" on page 21.
   - If yes, this problem is not one of the common ones that cause this issue. Contact Adobe Support.

J2CA0294W warning messages

To avoid receiving warning messages in the SystemOut.log file related to the deprecated usage of direct JNDI look-up, you can modify the WebSphere logging level.

To suppress the warning message "J2CA0294W" from the SystemOut.log, you can change the logging level to `*=info:com.ibm.ejs.j2c.ConnectionFactoryBuilderImpl=severe`.

➤ **To set the logging levels for your logs:**

1. Log in to WebSphere Administrative Console using the URL http://*[hostname]*:9060/admin.
2. In the WebSphere Administrative Console navigation tree, click **Servers** > ***server1*** > **Logging and Tracing** > **JVM Logs** > **Change Log Detail Levels**.
3. On the **Configuration** tab, type the following string:

   ```
   *=info: com.ibm.ejs.j2c.ConnectionFactoryBuilderImpl=severe
   ```

4. Click **OK** and then, in the **Messages** box, click **Save directly to Master Configuration**.

Exceptions thrown when initializing the LiveCycle ES database multiple times

When you initialize the LiveCycle ES database after it has already been initialized, exceptions may be thrown, indicating that the POF schema has not been initialized. You can ignore this error.

LiveCycle Policy Server to LiveCycle Rights Management ES

If a computer crashes unexpectedly while migrating essential data (policies and database information) or non-essential data (such as audit events) and a reboot is required, the upgrade process will fail until several corrupted files are deleted. When the upgrade is run again, LiveCycle Configuration Manager quits when you begin the data migration and displays the following message:

```
java.io.StreamCorruptedException: invalid stream header
```

To avoid this problem, delete all files in C:\Adobe\LiveCycle8\configurationManager\working\upgrade with a file name that starts with Intermediate or OrigExported. For example, the following files should be deleted, and there will likely be more:

- Intermediate_NonCrit_APS_Audit.data
- Intermediate_NonCrit_APS_Audit.index
- Intermediate_NonCrit_APS_Audit.metadata
- OrigExported_NonCrit_APS_Audit.data
- OrigExported_NonCrit_APS_Audit.index
- OrigExported_NonCrit_APS_Audit.metadata

Additional upgrade issues

There are some issues to be aware of when you have upgraded from LiveCycle 7.x to LiveCycle ES.

Maintaining printer setting for PDF Generator ES when connecting remotely

If you are running PDF Generator ES, the default printer on the LiveCycle ES server must be set to Adobe Printer. (This printer is installed when you install Acrobat.) If you connect remotely to the LiveCycle ES server using the Remote Desktop Connection in Windows, the default printer setting may be changed to the setting on the remote client. This causes native format conversions to fail. To ensure that the required printer setting is maintained when you connect remotely to LiveCycle ES running PDF Generator ES, you can deselect the Printers option on the Local Resources tab in the Windows Remote Desktop Connection utility.

➤ **To ensure LiveCycle ES server printer setting is used when connecting from a remote computer:**

1. In the Remote Desktop Connection window (**Start** > **All Programs** > **Accessories** > **Communications** > **Remote Desktop Connection**), click **Local Resources.** (If tabs do not appear on the window, click **Options**.)

2. Deselect **Printers** and click **Connect**.

LiveCycle Document Security 7.x APSProxy configuration settings not required

The APSProxy configuration settings described in LiveCycle Document Security 7.x documentation are no longer required in LiveCycle ES. Running separate instances of LiveCycle Document Security and LiveCycle Policy Server is no longer supported because these programs have been replaced by the Digital Signatures ES and Rights Management ES solution components within a service-oriented architecture.

Issues related to LiveCycle Forms

Default form settings are restored when upgrading from LiveCycle Forms 7.x without User Management and Administrator

When you upgrade from LiveCycle Forms 7.x (installed without User Management and Administrator), any forms settings you customized in the forms administration interface are lost, and the default form settings are restored. This occurs because these settings are not stored in a database. You must reset form settings using LiveCycle Administration Console.

Forms created with LiveCycle Designer 7.1 do not render in PDF mode with LiveCycle 7.0

Forms created with Designer 7.1 or later will not render in PDF mode with LiveCycle 7.0 because of differences in the render cache text. The message "Encoding 184 is not supported" is displayed. However, if this error occurs, you can disable the use of render cache in the XCI file.

```
<renderCache>
<enable>0</enable>
</rendercache>
```

Difference in PDF version of output files generated by LiveCycle Forms 7.2 and Forms ES for LiveCycle Designer 8.0 created files

When LiveCycle Forms 7.2 rendered documents, it used PDF version 1.6 for PDF forms and 1.5 for PDF documents. When these documents are rendered using LiveCycle ES, the PDF version is PDF 1.7 for PDF forms and PDF 1.5 for PDF documents.

Minor changes in calendar and digital signatures displayed when forms are rendered in HTML

When forms are rendered in HTML, some differences occur from LiveCycle 7.x to LiveCycle ES in the areas of Calendar Control and Digital Signatures for HTML.

If a form includes the date-time field, a calendar is now displayed next to the date/time field. If a form has a signature field, an option is now available to sign the form in HTML.

The PrintIVS.ear file is not compatible in LiveCycle ES

The PrintIVS.ear file from LiveCycle Print 7.x should not be deployed on the LiveCycle ES servers.

Processing signature fields in LiveCycle ES

Field MDP in forms created in Acrobat or LiveCycle Designer are not supported in LiveCycle ES.

LiveCycle Form Manager deadlines and reminders cannot execute during upgrade

When you are upgrading LiveCycle Form Manager to LiveCycle Workspace ES (part of LiveCycle Process Management ES), deadlines and reminders that are set to be sent during the upgrade process do not execute.

Any deadline or reminder that is set to be sent at a time that coincides with the server down time that occurs during the upgrade process (that is, when the LiveCycle 7.x server has been stopped but LiveCycle ES is not yet up and running) are lost and never sent. When the upgrade is complete (LiveCycle 7.x data has been migrated to LiveCycle ES) and the LiveCycle ES server is up and running, deadlines and reminders function as expected.

Index

A

accessing
- LiveCycle Administration Console 53
- solution component web applications 57
- User Management 56

Adobe Acrobat, installing for LiveCycle PDF Generator ES 15
Adobe LiveCycle Administration Console, accessing 53
Adobe LiveCycle Configuration Manager
- viewing log files 71

Adobe LiveCycle Document Security
- APSProxy configuration settings 74
- migrating HSM credentials 58

Adobe LiveCycle ES
- documentation resources 6
- installing 16

Adobe LiveCycle ES database
- exceptions on initializing 73
- troubleshooting 71

Adobe LiveCycle Forms
- pre-7.2 client applications 10
- upgrade issues 74

Adobe LiveCycle PDF Generator ES
- installing Acrobat 15
- maintaining printer settings when connecting remotely 74
- setting environment variables 67
- setting watched folder parameters 68

Adobe LiveCycle Reader Extensions ES
- accessing web application 57
- Rights credential 17

Adobe LiveCycle Rights Management ES web application 57
Adobe LiveCycle Workspace ES web application 57
Adobe User Management, accessing 56
applications, updating client 10
APSProxy configuration settings 74
automatic installation checklist 12

B

Business Activity Monitoring ES
- upgrading 55

C

checklists 12
class not found error 72
classpath, specifying 19
client applications, updating 10
component files, installing 15
Configuration Manager
- about 42

configuring
- *See also* installing
- about configuring LiveCycle ES 8
- Acrobat for LiveCycle PDF Generator ES 19
- LDAP 60
- Rights credential 17
- tasks 11
- WebSphere manually 21

conventions, path name 6
credential, Rights, configuring 17

D

DB2 database
- driver, installing 25

deleting working files 54
deploying
- *See also* configuring
- about deploying LiveCycle ES 8
- checklist for automatic deployment 12
- checklist for manual deployment 13
- LiveCycle ES on Linux or UNIX 16
- post-deployment activities 53
- tasks 11
- verifying deployment 53

directory, temporary 16
documentation resources 6

E

EAR files
- uninstalling 51

environment variables
- setting for LiveCycle PDF Generator ES 67
- setting JAVA_HOME 17, 19

error logs, viewing 19
error messages
- class not found 72
- J2CA0294W warning 73
- JNDI name not found 72

exceptions 73

H

Hardware Security Module (HSM) credentials, migrating 58

I

installing
- *See also* configuring
- about installing LiveCycle ES 8
- Acrobat for LiveCycle PDF Generator ES 15
- checklist for automatic installation 12
- checklist for manual installation 13
- DB2 driver 25
- LiveCycle ES 16
- LiveCycle ES to a Windows staging platform 16
- solution component files 15

J

J2CA0294W warning 73
JAR files, updating 10
Java 1.4 10
Java SDK 17
JAVA_HOME, setting 17, 19
JNDI name not found error 72
JVM system logs, viewing 71

L

LDAP, configuring 60
LiveCycle Configuration Manager
    performing a configuration 43
LiveCycle. *See* Adobe LiveCycle
log files
    errors, viewing 19
    LCM, viewing 71
    troubleshooting 71
log level, modifying for WebSphere 72

M

manually configuring WebSphere 21
Microsoft Office 15

N

naming conventions, file path 6
native application format conversion 15

O

optical character recognition (OCR) generation 15

P

printer settings for LiveCycle PDF Generator ES 74

Q

QPACs, updating 11

R

remote connection 74
Rights credential, configuring 17

S

signature fields 75
SOAP
    port, establishing for WebSphere 43
solution component files, installing 15

T

temporary directory 16
troubleshooting
    application server considerations 70
    database initialization considerations 71
    getting help 70
    installation considerations 70
    log files 71
Trust Store 17

U

um-client.jar 10
uninstalling
    EAR files 51
    LiveCycle ES 69
upgrading
    about 9
    BAM Server 55
    LiveCycle Policy Server to LiveCycle Rights Management ES 73
    post-deployment tasks 10

V

verifying the deployment 53
viewing
    application server log files 54
    error log files 19
    JVM system log files 71

W

watched folder, setting performance parameters for LiveCycle PDF Generator ES 68
web applications, accessing 57
WebSphere
    SOAP port, establishing 43
WebSphere, configuring manually 21
Windows staging platform 16
working files, deleting 54